PADRÃO INTERNACIONAL

ISO/IEC 17799

Tecnologia da Informação – Código de Prática para Gestão da Segurança de Informações

Número de referência

ISO/IEC 17799:2000 (E)

Índice

Prefácio

A ISO (International Organization for Standardization) e a IEC (International Electrotechnical Commission) formam o sistema especializado para padronização mundial. Entidades nacionais que são membros da ISO ou IEC participam do desenvolvimento de Padrões Internacionais através de comitês técnicos estabelecidos pela respectiva organização para lidar com campos específicos de atividade técnica. Os comitês técnicos da ISO e da IEC colaboram em campos de interesse mútuo. Outras organizações internacionais, governamentais e não-governamentais, em associação com a ISO e a IEC, também participam dos trabalhos.

Os Padrões Internacionais são esboçados de acordo com as regras estabelecidas nas Diretivas ISO/IEC, Parte 3.

No campo da tecnologia da informação, a ISO e a IEC estabeleceram um comitê técnico conjunto, ISO/IEC JTC 1. Rascunhos dos Padrões Internacionais adotados pelo comitê técnico conjunto são circulados nos órgãos nacionais para votação. A publicação como um Padrão Internacional exige a aprovação de pelo menos 75% dos órgãos nacionais votantes.

Chamamos a atenção para a possibilidade de que alguns dos elementos deste Padrão Internacional podem estar sujeitos a direitos de patente. A ISO e a IEC não serão consideradas responsáveis pela identificação de todos ou quaisquer destes direitos de patente.

O Padrão Internacional ISO/IEC 17799 foi preparado pelo British Standards Institution (como BS 7799) e foi adotado, através de um procedimento especial de "regime de urgência", pelo Comitê Técnico Conjunto ISO/IEC JTC 1, *Tecnologia da Informação*, em paralelo à sua aprovação pelos órgãos nacionais da ISO e da IEC.

Introdução

O que é segurança de informações?

Informações são ativos que, como qualquer outro ativo importante para os negócios, possuem valor para uma organização e consequentemente precisam ser protegidos adequadamente. A segurança de informações protege as informações contra uma ampla gama de ameaças, para assegurar a continuidade dos negócios, minimizar prejuízos e maximizar o retorno de investimentos e oportunidades comerciais.

As informações podem existir sob muitas formas. Podem ser impressas ou escritas em papel, armazenadas eletronicamente, enviadas pelo correio ou usando meios eletrônicos, mostradas em filmes, ou faladas em conversas. Qualquer que seja a forma que as informações assumam, ou os meios pelos quais sejam compartilhadas ou armazenadas, elas devem ser sempre protegidas adequadamente.

A segurança de informações é aqui caracterizada como a preservação de:

a) confidencialidade: garantir que as informações sejam acessíveis apenas àqueles autorizados a terem acesso;

b) integridade: salvaguardar a exatidão e inteireza das informações e métodos de processamento;

c) disponibilidade: garantir que os usuários autorizados tenham acesso às informações e ativos associados quando necessário.

A segurança das informações é obtida através da implementação de um conjunto adequado de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software. Esses controles precisam ser estabelecidos para assegurar que os objetivos de segurança específicos da organização sejam alcançados.

Por que é necessária a segurança de informações

As informações e os processos, sistemas e redes que lhes dão suporte são ativos importantes para os negócios. A confidencialidade, a integridade e a disponibilidade das informações podem ser essenciais para manter a competitividade, o fluxo de caixa, a rentabilidade, o atendimento à legislação e a imagem comercial.

Cada vez mais, as organizações e seus sistemas de informação e redes enfrentam ameaças de segurança vindas das mais diversas fontes, incluindo fraudes através de computadores, espionagem, sabotagem, vandalismo, incêndio ou enchentes. Fontes de prejuízos tais como vírus de computador, *hackers* e ataques de negação de serviços têm se tornado mais comuns, mais ambiciosos e cada vez mais sofisticados.

Devido à dependência de sistemas e serviços de informação, as organizações estão mais vulneráveis às ameaças contra a segurança. A interconexão de redes públicas e privadas e o compartilhamento de recursos de informação aumentam a dificuldade de se conseguir controle de acesso. A tendência ao processamento distribuído vem enfraquecendo a efetividade do controle central especializado.

Muitos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser obtida através de meios técnicos é limitada, e deveria ser apoiada por

procedimentos e gestão adequados. Identificar quais controles devem ser implementados exige um planejamento cuidadoso e atenção aos detalhes. A gestão da segurança de informações precisa, no mínimo, da participação de todos os empregados da organização. Também pode exigir a participação de fornecedores, clientes ou acionistas. Consultoria especializada de organizações externas também pode ser necessária.

Os controles para segurança das informações são consideravelmente mais baratos e mais eficazes se incorporados no estágio de especificação de necessidades e projeto.

Como estabelecer os requisitos de segurança

É essencial que uma organização defina seus requisitos de segurança. Existem três fontes principais.

A primeira fonte é derivada da avaliação dos riscos contra a organização. Através da avaliação de riscos as ameaças aos ativos são identificadas, a vulnerabilidade e a probabilidade de ocorrência são avaliadas e o impacto potencial é estimado.

A segunda fonte são as exigências legais, estatutárias, regulamentadoras e contratuais que uma organização, seus parceiros comerciais, empreiteiros e fornecedores de serviços precisam atender.

A terceira fonte é o conjunto específico de princípios, objetivos e requisitos para processamento de informações que uma organização desenvolveu para dar suporte a suas operações.

Avaliando os riscos de segurança

Os requisitos de segurança são identificados através de uma avaliação metódica dos riscos de segurança. Os gastos com controles precisam ser pesados contra os prováveis prejuízos resultantes de falhas na segurança. Técnicas de avaliação de riscos podem ser aplicadas a toda a organização, ou apenas a partes dela, bem como a sistemas de informação individuais, componentes de sistemas específicos ou serviços onde isto for praticável, realístico e útil.

A avaliação de riscos é a consideração sistemática de:

a) o provável prejuízo ao negócio resultante de uma falha de segurança, levando em conta as conseqüências potenciais de uma perda de confiabilidade, integridade ou disponibilidade das informações e outros ativos;

b) a probabilidade realística de tais falhas ocorrerem sob a luz de ameaças e vulnerabilidades prevalecentes, e os controles atualmente implementados.

Os resultados desta avaliação ajudarão a guiar e determinar a ação gerencial adequada e as prioridades para gerir os riscos de segurança de informação, e para implementar controles selecionados para proteger contra esses riscos. O processo de avaliar riscos e selecionar controles pode precisar ser executado diversas vezes para cobrir diferentes partes da organização ou sistemas de informação individuais.

É importante executar revisões periódicas dos riscos de segurança e dos controles implementados para:

a) levar em conta as mudanças nas prioridades e necessidades do negócio;

b) considerar novas ameaças e vulnerabilidades;

c) confirmar que os controles permanecem eficazes e apropriados.

As revisões devem ser executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações anteriores e das mudanças nos níveis de riscos que a gerência está preparada para aceitar. As avaliações de riscos freqüentemente são executadas primeiro em um nível superior, como uma forma de priorizar recursos nas áreas de alto risco, e depois em um nível mais detalhado, para tratar riscos específicos.

Selecionando controles

Uma vez que os requisitos de segurança tenham sido identificados, devem ser selecionados e implementados controles para garantir que os riscos sejam reduzidos a um nível aceitável. Os controles podem ser selecionados a partir deste documento, ou de outros conjuntos de controles, ou novos controles podem ser projetados para satisfazer necessidades específicas, conforme apropriado. Existem muitas formas diferentes de gerenciar riscos e este documento fornece exemplos de enfoques comuns. Entretanto, é necessário reconhecer que alguns desses controles não são aplicáveis a todos os sistemas de informação ou ambientes, e podem não ser praticáveis para todas as organizações. Por exemplo, o item 8.1.4 descreve como as tarefas podem ser segregadas para impedir fraudes ou erros. Pode não ser possível para pequenas organizações segregar todas as tarefas e podem ser necessárias outras formas para se obter o mesmo objetivo de controle. Como um outro exemplo, os itens 9.7 e 12.1 descrevem como o uso de sistemas pode ser monitorado e como podem ser coletadas provas. Os controles descritos, como gravação de *log* de eventos, podem conflitar com a legislação aplicável, tal como proteção da privacidade para clientes ou no local de trabalho.

Os controles devem ser selecionados considerando o custo de implementação em relação aos riscos que se quer reduzir e aos prejuízos potenciais se ocorrer uma quebra de segurança. Fatores não monetários, tais como perda de reputação, também devem ser levados em conta.

Alguns dos controles neste documento podem ser considerados como princípios orientadores para a gestão da segurança de informações e podem ser aplicáveis à maioria das organizações. Eles são explicados mais detalhadamente a seguir, no tópico “Ponto de partida para a segurança das informações”.

Ponto de partida para a segurança das informações

Vários controles podem ser considerados como princípios orientadores que fornecem um bom ponto de partida para implementação da segurança de informações. Eles são ou baseados nas exigências essenciais da legislação ou considerados como a melhor prática comum para a segurança de informações.

Os controles considerados como essenciais para uma organização, do ponto de vista legal, incluem:

a) proteção de dados e privacidade de informações pessoais (ver item 12.1.4);

b) salvaguarda de registros organizacionais (ver 12.1.3);

c) direitos de propriedade intelectual (ver 12.1.2).

Os controles considerados como a melhor prática comum para segurança de informações incluem:

a) documento de política de segurança de informações (ver 3.1);
b) alocação de responsabilidades quanto à segurança das informações (ver 4.1.3);
c) educação e treinamento para segurança das informações (ver 6.2.1);
d) relatórios dos incidentes de segurança (ver 6.3.1);
e) gerenciamento da continuidade do negócio (ver 11.1).

Esses controles se aplicam à maioria das organizações e dos ambientes. Deve-se observar que, apesar de os controles neste documento serem importantes, a relevância de qualquer controle deve ser determinada sob a luz dos riscos específicos que uma organização está enfrentando. Portanto, apesar de o enfoque acima ser considerado um bom ponto de partida, ele não substitui uma seleção de controles baseada em uma avaliação de riscos.

Fatores críticos para o sucesso

A experiência tem mostrado que os fatores seguintes freqüentemente são críticos para a implementação bem-sucedida da segurança de informações dentro de uma organização:

a) política, objetivos e atividades de segurança que reflitam os objetivos do negócio;
b) uma abordagem para implementar a segurança que seja consistente com a cultura organizacional;
c) suporte visível e compromisso por parte da administração;
d) um bom entendimento das necessidades de segurança, avaliação de riscos e gerenciamento de riscos;
e) marketing de segurança eficaz para todos os gerentes e empregados;
f) distribuição de orientação sobre a política e os padrões de segurança de informação para todos os empregados e contratados;
g) fornecimento de treinamento e educação apropriados;
h) um sistema abrangente e balanceado de medição, usado para avaliar o desempenho na gestão de segurança de informações e sugestões de *feedback* para melhorias.

Desenvolvendo suas próprias diretrizes

Este código de prática pode ser considerado como um ponto de partida para desenvolver orientação específica para a organização. Pode ser que nem todos os controles e diretrizes deste código de prática sejam aplicáveis. Além disso, controles adicionais não incluídos neste documento podem ser necessários. Quando isto acontece, pode ser útil reter referências cruzadas que facilitarão a verificação do cumprimento das exigências por auditores e parceiros comerciais.

Tecnologia da Informação - Código de Prática para Gestão da Segurança de Informações

1 Escopo

Este padrão faz recomendações para a gestão da segurança de informações para uso daqueles que são responsáveis por iniciar, implementar ou manter a segurança em suas organizações. Intenciona fornecer uma base comum para o desenvolvimento de padrões de segurança organizacional e práticas eficazes de gestão de segurança de informações e fornecer confiança nos intercâmbios inter-organizacionais. As recomendações deste padrão devem ser selecionadas e usadas de acordo com as leis e regulamentos aplicáveis.

2 Termos e definições

Para os propósitos deste documento, as definições seguintes se aplicam:

2.1 Segurança de informações

Preservação da confidencialidade, integridade e disponibilidade das informações.

- **Confidencialidade**
  Garantir que as informações sejam acessíveis apenas para aqueles que estão autorizados a acessá-las.

- **Integridade**
  Salvaguardar a exatidão e a inteireza das informações e métodos de processamento.

- **Disponibilidade**
  Assegurar que os usuários autorizados tenham acesso às informações e aos ativos associados quando necessário.

2.2 Avaliação de riscos

Avaliação das ameaças às informações e às facilidades[1] de processamento de informações, dos impactos nas informações e nas facilidades, das vulnerabilidades das informações e facilidades, e da probabilidade de ocorrência de tais riscos.

2.3 Gestão de riscos

Processo de identificar, controlar e minimizar ou eliminar os riscos de segurança que podem afetar sistemas de informações, a um custo aceitável.

[1] N.T.: A palavra inglesa “facilities” significa “recursos, meios, comodidades, instalações”. Neste documento foi traduzida como *facilidades*, com o significado de “meios prontos de se conseguir algo, de se chegar a um fim”.

3 Política de segurança

3.1 Política de segurança de informações

Objetivo: Fornecer direção e apoio gerenciais para a segurança de informações. A gerência deve estabelecer uma direção política clara e demonstrar suporte a, e comprometimento com, a segurança das informações através da emissão e manutenção de uma política de segurança de informações para toda a organização.

3.1.1 Documento da política de segurança de informações

Um documento com a política deve ser aprovado pela gerência, publicado e divulgado, conforme apropriado, para todos os empregados. Ele deve declarar o comprometimento da gerência e estabelecer a abordagem da organização quanto à gestão da segurança de informações. No mínimo, a seguinte orientação deve ser incluída:

a) uma definição de segurança de informações, seus objetivos gerais e escopo e a importância da segurança como um mecanismo capacitador para compartilhamento de informações (ver introdução);

b) uma declaração de intenção da gerência, apoiando os objetivos e princípios da segurança de informações;

c) uma breve explanação das políticas, princípios e padrões de segurança e das exigências a serem obedecidas que são de particular importância para a organização, por exemplo:

   1) obediência às exigências legislativas e contratuais;
   2) necessidades de educação (treinamento) para segurança;
   3) prevenção e detecção de vírus e outros softwares prejudiciais;
   4) gerenciamento da continuidade do negócio;
   5) conseqüências das violações da política de segurança;

d) uma definição das responsabilidades gerais e específicas pela gestão da segurança das informações, incluindo relatórios de incidentes de segurança;

e) referências a documentos que podem apoiar a política, por exemplo políticas de segurança mais detalhadas e procedimentos para sistemas de informação específicos ou regras de segurança que os usuários devem obedecer.

Esta política deve ser comunicada em toda a organização para os usuários de uma forma que seja relevante, acessível e entendível para o leitor-alvo.

3.1.2 Revisão e avaliação

A política deve ter um encarregado que seja responsável por sua manutenção e revisão de acordo com um processo de revisão definido. Esse processo deve assegurar que seja executada uma revisão em resposta a quaisquer mudanças que afetem a base da avaliação de riscos original, por exemplo incidentes de segurança significativos, novas vulnerabilidades ou mudanças na infra-estrutura organizacional ou técnica. Também devem ser programadas revisões periódicas dos seguintes aspectos:

a) a eficácia da política, demonstrada pela natureza, quantidade e impacto dos incidentes de segurança reportados;

b) o custo e impacto dos controles na eficiência do negócio;

c) os efeitos das mudanças na tecnologia.

4 Segurança organizacional

4.1 Infra-estrutura para segurança de informações

Objetivo: Gerenciar a segurança das informações dentro da organização.

Deve ser estabelecida uma estrutura gerencial para iniciar e controlar a implementação da segurança de informações dentro da organização.

Foros gerenciais adequados com liderança da administração devem ser estabelecidos para aprovar a política de segurança de informações, atribuir papéis de segurança e coordenar a implementação da segurança em toda a organização. Se necessário, um canal de aconselhamento especializado em segurança de informações deve ser estabelecido e disponibilizado dentro da organização. Contatos com especialistas em segurança externos devem ser desenvolvidos para acompanhar as tendências da indústria, monitorar padrões e métodos de avaliação e prover pontos de contato adequados para quando se lidar com incidentes de segurança. Um enfoque multidisciplinar quanto à segurança de informações deve ser encorajado; por exemplo, envolvendo a cooperação e colaboração de gerentes, usuários, administradores, projetistas de aplicações, auditores e equipe de segurança e especialistas em áreas tais como seguro e gestão de riscos.

4.1.1 Fórum gerencial de segurança de informações

Segurança de informações é uma responsabilidade corporativa compartilhada por todos os membros da equipe gerencial. Portanto, deve ser considerado um fórum gerencial para assegurar a existência de direção clara e suporte visível por parte da gerência para as iniciativas de segurança. Esse fórum deve promover a segurança dentro da organização através de comprometimento apropriado e alocação de recursos adequados. O fórum pode ser parte de um corpo gerencial existente. Geralmente, tal fórum encarrega-se do seguinte:

a) revisar e aprovar a política de segurança de informações e responsabilidades gerais;

b) monitorar mudanças significativas na exposição dos ativos de informação às principais ameaças;

c) revisar e monitorar incidentes que afetem a segurança das informações;

d) aprovar as iniciativas importantes para aprimorar a segurança das informações.

Um gerente deve ser responsável por todas as atividades relacionadas com a segurança.

4.1.2 Coordenação da segurança de informações

Em uma organização de grande porte, pode ser necessário um fórum interfuncional de representantes das gerências de setores relevantes da organização para coordenar a implementação de controles de segurança de informação. Geralmente, um fórum desse tipo:

a) concorda sobre papéis e responsabilidades específicos para segurança de informações em toda a organização;
b) concorda sobre metodologias e processos específicos para segurança de informações, por exemplo avaliação de riscos e sistema de classificação de segurança;
c) concorda com e apoia iniciativas de segurança de informação que abrangem toda a organização; por exemplo, programas de conscientização sobre segurança;
d) assegura que a segurança seja parte do processo de planejamento de informações;
e) avalia a adequação e coordena a implementação de controles específicos para segurança de informações em novos sistemas ou serviços;
f) revisa os incidentes relacionados com a segurança de informações;
g) promove a visibilidade do suporte corporativo para a segurança de informações em toda a organização.

4.1.3 Alocação de responsabilidades pela segurança das informações

As responsabilidades pela proteção de ativos individuais e pela condução de processos de segurança específicos devem ser claramente definidas.

A política de segurança de informações (ver cláusula 3) deve fornecer orientação geral sobre a alocação de papéis e responsabilidades relacionados à segurança na organização. Isto deve ser suplementado, onde necessário, com orientação mais detalhada para *sites*, sistemas ou serviços específicos. As responsabilidades locais pelos ativos físicos individuais e ativos de informação e processos de segurança, tais como o planejamento da continuidade do negócio, devem ser claramente definidas.

Em muitas organizações, um gerente de segurança de informações será designado para assumir a responsabilidade geral pelo desenvolvimento e implementação da segurança e para dar suporte à identificação dos controles.

Entretanto, a responsabilidade pela alocação de recursos e implementação dos controles freqüentemente permanecerá com gerentes individuais. Uma prática comum é apontar um proprietário para cada ativo de informação, o qual se tornará então responsável pela sua segurança no dia-a-dia.

Os proprietários dos ativos de informação podem delegar suas responsabilidades de segurança para gerentes individuais ou provedores de serviço. Não obstante, o proprietário permanece como responsável último pela segurança do ativo e deve ser

capaz de determinar se qualquer responsabilidade delegada foi desempenhada corretamente.

É essencial que as áreas pelas quais cada gerente é responsável sejam claramente definidas; em especial, deve ocorrer o seguinte:

a) Os vários ativos e processos de segurança associados com cada sistema individual devem ser identificados e claramente definidos.

b) Deve haver concordância quanto ao gerente responsável por cada ativo ou processo de segurança e os detalhes dessa responsabilidade devem ser documentados.

c) Os níveis de autorização devem ser claramente definidos e documentados.

4.1.4 Processo de autorização para facilidades de processamento de informações

Um processo gerencial de autorização para novas facilidades de processamento de informações deve ser implantado.

Os seguintes controles devem ser considerados:

a) novas facilidades devem ter a aprovação gerencial apropriada, autorizando seus propósitos e uso. Também deve ser obtida aprovação do gerente responsável pela manutenção do ambiente local de segurança de sistemas de informação para assegurar que todas as políticas relevantes e exigências sejam atendidas.

b) Quando necessário, o hardware e o software devem ser verificados para assegurar que eles são compatíveis como outros componentes do sistema.

   Nota: Aprovação de tipo pode ser exigida para certas conexões.

c) O uso de facilidades pessoais de processamento de informações para processar informações do negócio e quaisquer controles necessários têm que ser autorizados.

d) O uso de facilidades pessoais de processamento de informações no local de trabalho pode acarretar novas vulnerabilidade e portanto deve ser avaliado e autorizado.

Estes controles são especialmente importantes em ambientes que utilizam redes.

4.1.5 Aconselhamento especializado sobre segurança de informações

É muito provável que um aconselhamento especializado sobre segurança de informações seja necessário em muitas organizações. Idealmente, um consultor interno experiente em segurança de informações poderia prover isto. Nem todas as organizações podem desejar empregar um consultor especializado. Em tais casos, é recomendado que um indivíduo específico seja apontado para coordenar o conhecimento e as experiências internas para garantir consistência e ajudar na tomada de decisões relativas à segurança. Eles também deveriam ter acesso a consultores externos adequados que fornecessem aconselhamento especializado para situações que estejam fora da experiência própria interna.

Os consultores de segurança de informação, ou pontos de contato equivalentes, devem ter como tarefa fornecer aconselhamento sobre todos os aspectos da segurança de informações, usando ou seu próprio conselho ou externo. A qualidade de suas avaliações sobre as ameaças à segurança e de seu aconselhamento sobre os controles determinarão a efetividade da segurança de informações na organização. Para máxima eficácia e impacto, eles devem ter acesso direto às gerências em toda a organização.

O consultor de segurança de informações, ou ponto de contato equivalente, deve ser consultado o mais cedo possível em seguida a uma suspeita de incidente ou quebra de segurança para atuar como uma fonte de orientação especializada ou recursos investigativos. Apesar de a maioria das investigações internas de segurança serem conduzidas sob o controle da gerência, o consultor em segurança de informações pode ser chamado para aconselhar, liderar ou conduzir a investigação.

4.1.6 Cooperação entre organizações

Contatos apropriados com autoridades policiais, órgãos regulamentadores, provedores de serviços de informação e operadoras de telecomunicações devem ser mantidos para garantir que a ação apropriada seja tomada rapidamente, e obtido aconselhamento, na eventualidade de um incidente de segurança. Similarmente, deve ser considerada a afiliação a grupos de segurança e fóruns da indústria.

O intercâmbio de informações de segurança deve ser restrito para assegurar que informações confidenciais da organização não sejam repassadas para pessoas não autorizadas.

4.1.7 Revisão independente da segurança das informações

O documento sobre a política de segurança de informações (ver 3.1) estabelece a política e as responsabilidades pela segurança das informações. Sua implementação deve ser revisada de forma independente para fornecer garantia de que as práticas da organização refletem adequadamente a política, e que ela é viável e eficaz (ver 12.2).

Tal revisão pode ser executada pela função de auditoria interna, por um gerente independente ou por uma organização externa especializada em tais revisões, onde esses candidatos tenham as competências e experiências apropriadas.

4.2 Segurança para o acesso de terceiros

Objetivo: Manter a segurança das facilidades de processamento de informações organizacionais e ativos de informação acessados por terceiros.

O acesso por terceiros às facilidades de processamento de informações da organização deve ser controlado.

Onde houver uma necessidade do negócio para tal acesso de terceiros, deve ser efetuada uma avaliação de riscos para determinar as implicações de segurança e as exigências de controle. Os controles devem ser acordados e definidos em um contrato com a terceira parte.

O acesso de terceiros também pode envolver outros participantes. Contratos que permitem o acesso de terceiros devem incluir permissão para designação de outros participantes elegíveis e as condições para o acesso deles.

Esse padrão pode ser usado como uma base para tais contratos e ao se considerar a terceirização do processamento de informações.

4.2.1 Identificação dos riscos no acesso de terceiros

4.2.1.1 *Tipos de acesso*

O tipo de acesso concedido a uma terceira parte é de especial importância. Por exemplo, os riscos de acesso através de uma conexão de rede são diferentes dos riscos resultantes do acesso físico. Os tipos de acesso que devem ser considerados são:

a) acesso físico; por exemplo, a escritórios, salas de computadores, arquivos;

b) acesso lógico; por exemplo, aos bancos de dados e sistemas de informação da organização.

4.2.1.2 *Razões para o acesso*

O acesso de terceiros pode ser concedido por diversas razões. Por exemplo, existem empresas que fornecem serviços para uma organização e não estão localizadas *on-site* mas podem receber permissão de acesso físico e lógico, tais como:

a) equipe de suporte de hardware e software, que precisam acessar funcionalidades de aplicações no nível de sistema ou em baixo nível;

b) parceiros comerciais ou *joint-ventures*, que podem intercambiar informações, acessar sistemas de informações ou compartilhar bancos de dados.

Informações podem ser colocadas em risco pelo acesso por terceiros com uma gestão inadequada de segurança. Onde existir uma necessidade do negócio para conectar com uma instalação de terceiros, deve ser conduzida uma avaliação de riscos para identificar quaisquer necessidades de controles específicos. Deve ser levado em conta o tipo de acesso requerido, o valor das informações, os controles empregados pela terceira parte e as implicações desse acesso para a segurança das informações da organização.

4.2.1.3 *Terceiros on-site*

Terceiros que se localizam *on-site* por um período de tempo definido em seus contratos também podem provocar vulnerabilidades na segurança. Exemplos de terceiros *on-site* incluem:

a) equipe de suporte e manutenção de hardware e software;

b) serviços de limpeza, alimentação, guardas de segurança e outros serviços de apoio terceirizados;

c) colocação de estudantes (estagiários) e outros contratos casuais de curto prazo;

d) consultores.

É essencial entender que são necessários controles para administrar o acesso de terceiros às facilidades de processamento de informações. Geralmente, todas as exigências de segurança resultantes do acesso de terceiros ou controles internos devem ser refletidos pelo contrato com a terceira parte (ver também 4.2.2). Por

exemplo, se existir uma necessidade especial quanto à confidencialidade das informações, contratos de não divulgação podem ser usados (ver 6.1.3).

O acesso às informações e às facilidades de processamento de informações por terceiras partes não deve ser concedido até que os controles adequados tenham sido implementados e tenha sido assinado um contrato definindo os termos para a conexão ou acesso.

4.2.2 Requisitos de segurança para contratos com terceiros

Os arranjos que envolvem o acesso de terceiras partes às facilidades de processamento de informações da organização devem ser baseados em um contrato formal contendo, ou referenciando, todos os requisitos de segurança para garantir a obediência às políticas e padrões de segurança da organização. O contrato deve garantir que não haja mal-entendidos entre a organização e a terceira parte. As organizações devem se satisfazer quanto à idoneidade de seu fornecedor. Os seguintes termos devem ser considerados para inclusão no contrato:

a) a política geral de segurança das informações;

b) a proteção de ativos, incluindo:
   1) procedimentos para proteger ativos da organização, incluindo informações e software;
   2) procedimentos para determinar se ocorreu qualquer comprometimento dos ativos, por exemplo perda ou modificação de dados
   3) controles para garantir a devolução ou destruição de informações e ativos no final do contrato, ou em algum momento acordado durante o contrato;
   4) integridade e disponibilidade;
   5) restrições à cópia e divulgação de informações;

c) uma descrição de cada serviço a ser disponibilizado;

d) o nível desejado de serviço e níveis de serviço não aceitáveis;

e) provisão para transferência de equipe onde apropriado;

f) as respectivas responsabilidades das partes com relação ao contrato;

g) as responsabilidades relacionadas com aspectos legais; por exemplo, legislação de proteção de dados, especialmente considerando diferentes sistemas legais nacionais se o contrato envolver a cooperação com organizações em outros países (ver também 12.1);

h) direitos de propriedade intelectual (IPRs) e atribuição de *copyrights* (ver 12.1.2) e proteção de qualquer trabalho colaborativo (ver também 6.1.3);

i) acordos para o controle de acesso, cobrindo:
   1) os métodos de acesso permitidos, e o controle e o uso de identificadores únicos, tais como IDs de usuário e senhas;
   2) um processo de autorização para acesso de usuários e privilégios;
   3) uma exigência de manter uma lista de indivíduos autorizados a usar os serviços que estão sendo disponibilizados e quais são seus direitos e privilégios com respeito a tal uso;

j) a definição de critérios de desempenho verificáveis, sua monitoração e relatórios;

k) o direito de monitorar, e revogar, as atividades dos usuários;

l) o direito de auditar responsabilidades contratuais ou de realizar tais auditorias por meio de uma terceira parte;

m) o estabelecimento de um processo de escalonamento para resolução de problemas; providências de contingência também devem ser consideradas onde apropriado;

n) responsabilidades relacionadas com instalação e manutenção de hardware e software;

o) uma estrutura clara para relatórios informativos e formatos acordados de relatórios;

p) um processo claro e especificado de troca de gerência;

q) quaisquer controles de proteção física necessários e mecanismos para assegurar que esses controles sejam obedecidos;

r) treinamento de administradores e usuários nos métodos, procedimentos e segurança;

s) controles para assegurar a proteção contra software malicioso (ver 8.3);

t) arranjos para reportar, notificar e investigar incidentes de segurança e quebras de segurança;

u) envolvimento da terceira parte com subcontratados.

4.3 *Outsourcing*

Objetivo: Manter a segurança das informações quando a responsabilidade pelo processamento das informações tiver sido terceirizada com outra organização. Os acordos de terceirização *(outsourcing)* devem tratar dos riscos, controles de segurança e procedimentos para sistemas de informações, ambientes de rede e/ou *desktop* no contrato entre as partes.

4.3.1 Requisitos de segurança em contratos de outsourcing

Os requisitos de segurança de uma organização que terceiriza a gestão e o controle de todos ou alguns de seus sistemas de informação, ambientes de redes e/ou ambientes de *desktop* devem ser tratados em um contrato acordado entre as partes.

Por exemplo, o contrato deve mencionar:

a) como as exigências legais serão satisfeitas; por exemplo, a legislação quanto à proteção de dados;

b) quais arranjos devem ser implantados para assegurar que todas as partes envolvidas na terceirização, incluindo subcontratados, estejam cientes de suas responsabilidades para com a segurança;

c) como a integridade e a confidencialidade dos ativos de informação da organização devem ser mantidos e testados;
d) quais controles físicos e lógicos serão usados para restringir e limitar o acesso às informações sensíveis da organização para os usuários autorizados;
e) como a disponibilidade dos serviços deve ser mantida na eventualidade de um desastre;
f) quais níveis de segurança física devem ser fornecidos para equipamento terceirizado;
g) o direito de auditoria.

Os termos relacionados na lista do item 4.2.2 também devem ser considerados como parte desse contrato. O contrato deve permitir que os requisitos e procedimentos de segurança sejam expandidos em um plano de gestão de segurança a ser acordado entre as partes.

Apesar de contratos de terceirização poderem apresentar algumas questões complexas de segurança, os controles incluídos neste código de prática podem servir como um ponto de partida para um acordo quanto à estrutura e o conteúdo do plano de gestão da segurança.

5 Classificação e controle dos ativos

5.1 Responsabilidade pelos ativos

Objetivo: Manter proteção apropriada para os ativos organizacionais. Todos os ativos de informação mais importantes devem ter um proprietário nominal, responsável por eles. A responsabilidade pelos ativos ajuda a assegurar que seja mantida uma proteção adequada. Os proprietários devem ser identificados para todos os ativos importantes e a responsabilidade pela manutenção dos controles apropriados deve ser atribuída. A responsabilidade pela implementação dos controles pode ser delegada. A responsabili-dade final deve permanecer com o proprietário designado do ativo.

5.1.1 Inventário dos ativos

Um inventário dos ativos ajuda a assegurar que ocorra uma proteção efetiva dos ativos, e também pode ser exigido para outros fins do negócio, tais como razões de salubridade e segurança, seguros ou razões financeiras (gestão de ativos). O processo de compilar um inventário de ativos é um aspecto importante da administração de riscos. Uma organização precisa ser capaz de identificar seus ativos e a importância e o valor relativos desses ativos. Baseado nessas informações, uma organização pode então prover níveis de proteção proporcionais ao valor e importância dos ativos. Deve ser levantado e mantido um inventário dos ativos importantes associados com cada sistema de informações. Cada ativo deve ser claramente identificado e sua propriedade e classificação de segurança (ver 5.2) devem ser acordadas e

documentadas, juntamente com sua localização atual (importante ao se tentar recuperar perda ou dano). Exemplos de ativos associados com sistemas de informação são:

a) ativos de informação: bancos de dados e arquivos de dados, documentação de sistemas, manuais de usuário, material de treinamento, procedimentos operacionais ou de suporte, planos de continuidade, arranjos de *fallback*[2], informações em *archives*[3];

b) ativos de software: software aplicativo, software básico, ferramentas de desenvolvimento e utilitários;

c) ativos físicos: equipamento de computador (processadores, monitores, laptops, modems), equipamentos de comunicação (roteadores, PABXs, aparelhos de fax, secretárias eletrônicas), mídia magnética (fitas e discos), outros equipamentos técnicos (geradores de energia, unidades de condicionamento de ar), móveis, acomodações;

d) serviços: serviços de informática e telecomunicações, serviços públicos em geral (aquecimento, iluminação, energia, ar-condicionado).

5.2 Classificação[4] das informações

Objetivo: Garantir que os ativos de informação recebam um nível de proteção adequado. As informações devem ser classificadas para indicar a necessidade, as prioridades e o grau de proteção. As informações apresentam graus variáveis de suscetibilidade e criticalidade. Alguns itens podem exigir um nível adicional de proteção ou tratamento especial. Um sistema de classificação das informações deve ser usado para definir um conjunto apropriado de níveis de proteção e comunicar a necessidade de medidas de tratamento especiais.

5.2.1. Diretrizes para a classificação

As classificações e controles associados de proteção para as informações devem considerar as necessidades do negócio quanto ao compartilhamento ou restrição das informações, e os impactos para o negócio associados com tais necessidades, por exemplo acesso não autorizado ou danos às informações. Em geral, a classificação dada às informações é um atalho para determinar como essas informações devem ser manipuladas e protegidas.

As informações e as saídas geradas pelos sistemas que tratam dados confidenciais devem ser rotuladas segundo seu valor e sensibilidade para a organização. Também

[2] N.T.: *Fallback*: o que pode ser usado quando falhar o suprimento, método ou atividade normal.
[3] N.T.: *Archive*: um conjunto de arquivos de computador compactados juntos para fins de *backup*, para serem transportados para outro local, para economizar espaço em disco ou por algum outro motivo. Um *archive* pode incluir uma simples lista de arquivos ou arquivos organizados sob uma estrutura de diretório ou catálogo.
[4] N.T.: A palavra inglesa *classification*, no contexto deste documento, significa "atribuição de grau de confidencialidade". A tradução usada, classificação, deve ser entendida da mesma forma.

pode ser apropriado rotular informações em termos de quão críticas elas são para a organização, por exemplo em termos de sua integridade e disponibilidade.

As informações freqüentemente deixam de ser sensíveis ou críticas após um certo período de tempo; por exemplo, quando as informações são tornadas públicas. Esses aspectos devem ser levados em conta, assim como também o fato de uma classificação excessiva poder levar a despesas adicionais desnecessárias. As diretrizes para classificação devem prever e admitir o fato de que a classificação de um item qualquer de informação não é necessariamente fixa por todo o tempo, e pode mudar de acordo com alguma política predeterminada (ver 9.1).

Deve-se levar em consideração a quantidade de categorias de classificação e os benefícios a serem obtidos com o seu uso. Esquemas excessivamente complexos podem ser incômodos e dispendiosos para uso ou se mostrarem pouco práticos. Deve-se tomar cuidado ao se interpretar rótulos de classificação em documentos vindos de outras organizações, as quais podem ter definições diferentes para rótulos iguais ou com denominação semelhante.

A responsabilidade pela definição da classificação de um item de informação, por exemplo para um documento, um registro de dados, um arquivo de dados ou disquete, e para revisar periodicamente aquela classificação, deve permanecer com o originador ou o proprietário designado da informação.

5.2.2 Rotulagem e manuseio de informações

É importante que um conjunto apropriado de procedimentos seja definido para rotulagem e manuseio das informações de acordo com o esquema de classificação adotado pela organização. Esses procedimentos precisam cobrir os ativos de informação nos formatos físicos e eletrônicos. Para cada classificação, os procedimentos de manuseio devem ser definidos para cobrir os seguintes tipos de atividades de processamento de informação:

a) cópia;

b) armazenamento;

c) transmissão pelo correio, fax e correio eletrônico;

d) transmissão verbal, incluindo telefone celular, correio de voz, secretárias eletrônicas;

e) destruição.

As saídas geradas pelos sistemas que contêm informações classificadas como sensíveis ou críticas devem portar um rótulo de classificação apropriado (na saída). O rótulo deve refletir a classificação de acordo com as regras estabelecidas no item 5.2.1. Os itens a serem considerados incluem relatórios impressos, exibições em tela, mídia gravada (fitas, discos, CDs, cassetes), mensagens eletrônicas e transferências de arquivos.

As etiquetas físicas são geralmente as formas mais apropriadas de rotulagem. Entretanto, alguns ativos de informação, tais como documentos sob a forma eletrônica, não podem ser fisicamente rotulados e é preciso usar meios eletrônicos de rotulagem.

6 Segurança relacionada ao pessoal

6.1 Segurança na definição de funções e alocação de pessoal

Objetivo: Reduzir os riscos de erros humanos, roubos, fraudes ou uso indevido das facilidades. As responsabilidades de segurança devem ser tratadas no estágio de recrutamento, incluídas em contratos e monitoradas durante o tempo que o indivíduo estiver no emprego. Os candidatos em potencial devem ser adequadamente selecionados (ver 6.1.2), especialmente para funções sensíveis. Todos os empregados e usuários terceirizados das facilidades de processamento de informações devem assinar um contrato de confidencialidade (não divulgação).

6.1.1 Incluindo a segurança nas responsabilidades dos serviços

Os papéis de segurança e as responsabilidades, conforme delineados na política de segurança de informações da organização (ver 3.1), devem ser documentados onde for apropriado. Eles devem incluir quaisquer responsabilidades gerais pela implementação ou manutenção da política de segurança bem como quaisquer responsabilidades específicas pela proteção de determinados ativos, ou pela execução de determinados processos ou atividades de segurança.

6.1.2 Seleção e política de pessoal

Para os empregados permanentes, no momento das propostas de emprego, devem ser efetuadas verificações de confirmação. Estas devem incluir os seguintes controles:

a) disponibilidade de referências satisfatórias sobre o caráter da pessoa, por exemplo uma referência profissional, outra pessoal;

b) uma verificação (quanto à veracidade e exatidão) do curriculum vitae do candidato;

c) confirmação das qualificações acadêmicas e profissionais declaradas;

d) verificação independente de identidade (passaporte ou documento similar).

Onde uma função, na contratação inicial ou na promoção, envolver a pessoa ter acesso às facilidades de processamento de informações, e em particular se essas lidarem com informações sensíveis (por exemplo, informações financeiras ou altamente confidenciais), a organização também deve executar uma verificação de crédito. Para empregados que detêm posições de considerável autoridade essa verificação deve ser repetida periodicamente.

Um processo de filtragem similar deve ser executado para contratados e empregados temporários. Quando essas pessoas forem fornecidas através de uma agência, o contrato com a agência deve especificar claramente as responsabilidades da agência na filtragem e os procedimentos de notificação que eles precisam seguir se a filtragem não for concluída ou se os resultados causarem dúvidas ou suspeitas.

A gerência deve avaliar a supervisão necessária para empregados novos e inexperientes que tenham autorização de acesso a sistemas sensíveis. O trabalho de toda a equipe deve estar sujeito à revisão periódica e a procedimentos de aprovação por um membro da equipe de nível sênior.

Os gerentes devem estar conscientes de que circunstâncias pessoais da equipe podem afetar seu trabalho. Problemas pessoais ou financeiros, alterações no comportamento ou estilo de vida, faltas recorrentes e evidência de stress ou depressão podem levar a fraudes, roubos, erros ou outras implicações de segurança. Essas informações devem ser tratadas de acordo com qualquer legislação apropriada existente na jurisdição relevante.

6.1.3 Contratos de confidencialidade

Contratos de confidencialidade ou não-divulgação são usados para avisar que informações são confidenciais ou secretas. Os empregados devem normalmente assinar tal contrato como parte de seus termos e condições iniciais de emprego.

Equipe temporária e usuários terceirizados que já não estejam cobertos por um contrato existente (contendo a cláusula de confidencialidade) devem ser obrigados a assinar um contrato de confidencialidade antes de terem concedido o acesso às facilidades de processamento de informações.

Os contratos de confidencialidade devem ser revisados quando houver alterações nas condições de emprego ou do contrato, particularmente quando os empregados forem deixar a organização ou os trabalhos temporários estiverem por terminar.

6.1.4 Termos e condições de emprego

Os termos e condições de emprego devem declarar a responsabilidade do empregado pela segurança das informações. Onde apropriado, essas responsabilidades devem continuar por um período definido após o término do vínculo de emprego. Deve ser incluída a ação a ser executada se o empregado desrespeitar as exigências de segurança.

As responsabilidades e direitos legais do empregado, por exemplo, com respeito a leis de *copyright* ou legislação de proteção de dados, devem ser esclarecidas e incluídas nos termos e condições do contrato de trabalho. A responsabilidade pela classificação e gerenciamento dos dados do empregado também deve ser incluída. Onde for apropriado, os termos e condições do contrato de trabalho devem declarar que aquelas responsabilidades continuam vigorando fora das instalações físicas da organização e fora das horas de trabalho normais, por exemplo no caso de trabalho em casa (ver também 7.2.5 e 9.8.1).

6.2 Treinamento dos usuários

Objetivo: Assegurar que os usuários se conscientizem das preocupações e ameaças à segurança das informações, e estejam equipados para apoiar a política de segurança organizacional no curso de seu trabalho normal.

Os usuários devem ser treinados nos procedimentos de segurança e no uso correto das facilidades de processamento de informações para minimizar os possíveis riscos de segurança.

6.2.1 Educação e treinamento sobre segurança de informações

Todos os empregados da organização e, onde for relevante, usuários terceirizados, devem receber treinamento apropriado e atualizações periódicas sobre as políticas e procedimentos organizacionais. Isto inclui as exigências de segurança, as responsabilidades legais e controles corporativos, bem como treinamento no uso correto das facilidades de processamento de informações, por exemplo, procedimento de *logon*, uso de pacotes de software, antes de serem autorizados a acessar informações ou serviços.

6.3 Respondendo a incidentes de segurança e mal funcionamentos

Objetivo: Minimizar os danos resultantes de incidentes de segurança e mal funcionamentos, e monitorar e aprender com tais incidentes.

Incidentes que afetam a segurança devem ser reportados através de canais administrativos apropriados o mais rapidamente possível.
Todos os empregados e contratados devem estar cientes dos procedimentos para reportar os diferentes tipos de incidente (quebra de segurança, ameaça, fraqueza ou mal funcionamento) que possam ter impacto na segurança dos ativos organizacionais. Deve ser exigido que eles reportem quaisquer incidentes observados ou suspeitados o mais rapidamente possível para o ponto de contato designado. A organização deve estabelecer um processo disciplinar formal para lidar com empregados que cometam quebras de segurança. Para que se seja capaz de tratar os incidentes adequadamente, pode ser necessário colher provas o mais cedo possível após a ocorrência (ver 12.1.7).

6.3.1 Reportando incidentes de segurança

Os incidentes de segurança devem ser reportados através dos canais administrativos adequados o mais rapidamente possível.

Um procedimento formal para relatar os incidentes deve ser estabelecido, juntamente com um procedimento de resposta ao incidente, estabelecendo a ação a ser executada no recebimento de um relatório de incidente. Todos os empregados e contratados devem estar cientes do procedimento para reportar incidentes de segurança, e deve-se exigir que reportem tais incidentes o mais rápido possível. Processos de *feedback* adequados devem ser implementados para garantir que aqueles que reportaram os incidentes sejam notificados dos resultados após o incidente ser investigado e encerrado. Esses incidentes podem ser usados em um treinamento de conscientização dos usuários (ver 6.2) como exemplos do que pode acontecer, de como responder a tais incidentes e de como evitá-los no futuro (ver também 12.1.7).

6.3.2 Reportando pontos fracos na segurança

Os usuários de serviços de informações devem ser obrigados a anotar e reportar quaisquer pontos fracos observados ou suspeitados, ou ameaças, aos sistemas e serviços. Eles devem reportar esses assuntos diretamente à sua gerência ou diretamente ao seu provedor de serviços o mais rapidamente possível. Os usuários devem ser informados de que eles não devem, em nenhuma circunstância, tentar

provar (testar) um ponto fraco suspeitado. Isso é para a própria proteção deles, já que testar falhas pode ser interpretado como uma potencial utilização indevida do sistema.

6.3.3 Reportando mal funcionamento de softwares

Devem ser estabelecidos procedimentos para reportar mal funcionamento de softwares. As seguintes ações devem ser consideradas:

a) Os sintomas do problema e quaisquer mensagens que apareçam na tela devem ser anotados.

b) O computador deve ser isolado, se possível, e o seu uso deve ser interrompido. O contato apropriado deve ser alertado imediatamente. Se o equipamento tiver que ser examinado, ele deve ser desconectado de quaisquer redes organizacionais antes de ser religado. Disquetes não devem ser transferidos para outros computadores.

c) O assunto deve ser imediatamente reportado ao gerente de segurança de informações.

Os usuários não devem tentar remover o software suspeito a menos que sejam autorizados a fazê-lo. A recuperação deve ser executada por pessoal adequadamente treinado e experiente.

6.3.4 Aprendendo com os incidentes

Devem existir mecanismos para capacitar a quantificação e o monitoramento dos tipos, volumes e custos dos incidentes e mal funcionamentos. Essas informações devem ser usadas para identificar incidentes ou mal funcionamentos recorrentes ou de alto impacto. Isso pode indicar a necessidade de controles aprimorados ou adicionais para limitar a freqüência, os danos e custos de futuras ocorrências, ou de serem considerados no processo de revisão da política de segurança (ver 3.1.2).

6.3.5 Processo disciplinar

Deve existir um processo disciplinar formal para empregados que tenham violado as políticas e procedimentos de segurança organizacionais (ver 6.1.4 e, para retenção de provas, ver 12.1.7). Tal processo pode atuar como um meio de intimidação para empregados que poderiam de outra forma se inclinar a desrespeitar os procedimentos de segurança. Adicionalmente, ele deve também assegurar um tratamento justo e correto para os empregados que sejam suspeitos de cometer quebras de segurança severas ou persistentes.

7 Segurança física e ambiental

7.1 Áreas de segurança

Objetivo: Impedir acesso não autorizado, danos ou interferência às instalações físicas e às informações da organização. As facilidades de processamento de informações sensíveis ou críticas para o negócio devem ser localizadas em áreas seguras, protegidas por um perímetro de segurança

definido, com barreiras de segurança apropriadas e controles de entrada. Elas devem ser fisicamente protegidas contra acesso não autorizado, danos e interferências.
A proteção fornecida deve ser compatível com os riscos identificados. Uma política de “mesas limpas” e “telas limpas” é recomendada para reduzir o risco de acesso não autorizado ou danos a papéis, mídia e facilidades de processamento de informações.

7.1.1 Perímetro de segurança física

Proteção física pode ser obtida criando-se diversas barreiras físicas em torno dos edifícios e das facilidades de processamento de informações da organização. Cada barreira estabelece um perímetro de segurança, cada um aumentando a proteção total fornecida. As organizações devem usar perímetros de segurança para proteger áreas que contenham facilidades de processamento de informações (ver 7.1.3). Um perímetro de segurança é alguma coisa que constitui uma barreira, tal como uma parede, um portão de entrada controlado por cartão ou um balcão de recepção com atendentes. A localização e a resistência de cada barreira depende dos resultados de uma avaliação de riscos.

As diretrizes e controles seguintes devem ser considerados e implementados onde apropriado:

a) O perímetro de segurança deve ser claramente definido.

b) O perímetro de um edifício ou *site* que contenha facilidades de processamento de informações deve ser fisicamente seguro (isto é, não deve haver brechas no perímetro ou áreas onde uma entrada forçada possa ocorrer com facilidade). As paredes externas do *site* devem ser de construção sólida e todas as portas externas devem ser adequadamente protegidas contra acesso não autorizado, com mecanismos de controle, barras, alarmes, trancas, etc.

c) Deve existir uma área de recepção com atendentes ou outros meios de controlar o acesso físico ao *site* ou ao edifício. O acesso aos *sites* ou edifícios deve ser restrito apenas ao pessoal autorizado.

d) As barreiras físicas devem, se necessário, ser estendidas do piso real ao teto real para impedir entrada não autorizada e contaminação ambiental, tais como as causadas por incêndio ou inundação.

e) Todas as portas corta-fogo em um perímetro de segurança devem ter alarmes e devem fechar fazendo barulho.

7.1.2 Controles para entrada física

As áreas de segurança devem ser protegidas por controles de entrada apropriados, para garantir que apenas o pessoal autorizado tenha acesso a elas. Os seguintes controles devem ser considerados:

a) Visitantes nas áreas de segurança devem ser supervisionados ou conduzidos pela segurança e as datas e horários de sua entrada e saída devem ser registrados. Eles devem ter seu acesso concedido apenas para propósitos específicos e autorizados e devem ser instruídos sobre os requisitos de segurança da área e sobre os procedimentos de emergência.

b) O acesso a informações sensíveis, e facilidades de processamento de informações, deve ser controlado e restringido apenas ao pessoal autorizado. Controles de autenticação, tais como cartões magnéticos com PIN, devem ser usados para autorizar e validar todos os acessos. Uma *audit trail*[5] de todos os acessos deve ser mantido em segurança.

c) Todo o pessoal deve ser obrigado a usar alguma forma visível de identificação e deve ser encorajado a questionar estranhos desacompanhados e qualquer um que não esteja usando identificação visível.

d) Os direitos de acesso às áreas de segurança devem ser revisados e atualizados regularmente.

7.1.3 Segurança nos escritórios, salas e instalações

Uma área de segurança pode ser um escritório trancado ou várias salas dentro de um perímetro de segurança física, o qual pode ser trancado e pode conter vários cofres ou armários trancados. A seleção e o projeto de uma área segura deve levar em conta a possibilidade de danos por incêndio, inundação, explosão, arruaças e outras formas de desastres naturais ou provocados. Deve-se considerar também os regulamentos e padrões relevantes quanto à saúde e segurança. Também devem ser levadas em consideração quaisquer ameaças à segurança apresentadas por locais vizinhos, como vazamento de água proveniente de outras áreas.

Os seguintes controles devem ser considerados:

a) As instalações principais devem ser situadas de modo a evitar o acesso pelo público.

b) Os edifícios devem ser discretos e dar a menor indicação possível de sua finalidade, sem sinais óbvios, internos e externos, que identifiquem a presença de atividades de processamento de informações.

c) Os equipamentos e funções de apoio, como fotocopiadoras e aparelhos de fax, devem ser situados apropriadamente dentro da área de segurança para evitar demandas para acesso, que poderiam comprometer informações.

d) Portas e janelas devem ser trancadas quando não houver ninguém presente e deve ser considerada uma proteção externa para as janelas, especialmente aquelas no andar térreo.

e) Sistemas adequados de detecção de invasão, instalados em padrões profissionais e testados regularmente, devem ser colocados para cobrir todas as portas externas e janelas acessíveis. Áreas desocupadas devem permanecer sempre com o alarme ligado. A cobertura deve também ser providenciada para outras áreas, como sala de computadores ou salas de telecomunicações.

f) As instalações de processamento de informações gerenciadas pela organização devem ser fisicamente separadas daquelas gerenciadas por terceiras partes.

g) Listas telefônicas internas, que identifiquem os locais das instalações de processamento de informações sensíveis, não devem ficar disponíveis para o público.

---

[5] N.T.: *Audit trail*: trilha para auditoria.

h) Materiais perigosos ou combustíveis devem ser armazenados a uma distância segura de uma área de segurança. Suprimentos volumosos, tal como papel, não devem ser armazenados dentro de uma área de segurança até serem necessários.

i) Equipamentos para *fallback* e mídia de *backup* devem ficar situados a uma distância segura para evitar danos provocados por um desastre no *site* principal.

7.1.4 Trabalhando em áreas de segurança

Controles e diretrizes adicionais podem ser necessários para aumentar a segurança de uma área de segurança. Isso inclui controles para os funcionários ou terceiros que trabalham na área de segurança, bem como atividades terceirizadas que sejam executadas lá. Os seguintes controles devem ser considerados:

a) Os funcionários devem estar cientes da existência de uma área de segurança, ou das atividades lá executadas, apenas na medida que for necessário que eles saibam.

b) Trabalho não supervisionado em áreas de segurança deve ser evitado, tanto por razões de segurança quanto para impedir oportunidades para atividades maliciosas.

c) Áreas de segurança vazias devem ficar fisicamente trancadas e serem periodicamente verificadas.

d) Para o pessoal terceirizado de serviços de apoio deve ser concedido acesso restrito às áreas de segurança ou instalações de processamento de informações sensíveis e apenas quando necessário. Esse acesso deve ser autorizado e monitorado. Barreiras adicionais e perímetros para controlar ao acesso físico podem ser necessárias entre áreas que tenham diferentes exigências de segurança dentro do perímetro de segurança.

e) Equipamentos fotográficos, de áudio, vídeo ou outras formas de gravação não devem ser permitidos, a não ser que sejam autorizados.

7.1.5 Áreas isoladas de carga e descarga

Áreas de carga e descarga devem ser controladas e, se possível, isoladas das facilidades de processamento de informações para evitar acesso não autorizado. Os requisitos de segurança de tais áreas devem ser determinados por uma avaliação de riscos. Os seguintes controles devem ser considerados:

a) O acesso a uma área de depósito a partir do exterior do prédio deve ser restrito a pessoal identificado e autorizado.

b) A área de depósito deve ser planejada de forma que os suprimentos possam ser descarregados sem que os entregadores ganhem acesso a outras partes do edifício.

c) As portas externas de uma área de depósito devem ser vigiadas quando a porta interna for aberta.

d) Os materiais recebidos devem ser inspecionados quanto a possíveis perigos [ver 7.2.1d)] antes de serem transferidos do depósito para o local de uso.

e) Os materiais recebidos devem ser registrados, se for o caso (ver 5.1), ao darem entrada no *site*.

7.2 Segurança dos equipamentos

Objetivo: Impedir perda, danos ou comprometimento de ativos e interrupção das atividades do negócio.

Os equipamentos devem ser fisicamente protegidos contra ameaças à segurança e perigos ambientais. A proteção dos equipamentos (incluindo aqueles usados *off-site*) é necessária para reduzir o risco de acesso não autorizado aos dados e para proteger contra perda ou danos. Também deve-se considerar a localização dos equipamentos e sua disposição física. Controles especiais podem ser necessários para proteger contra perigos ou acesso não autorizado, e para salvaguardar instalações de apoio, tais como suprimento de eletricidade e infra-estrutura de cabeamento.

7.2.1 Disposição física dos equipamentos e proteção

Os equipamentos devem ser protegidos, ou dispostos fisicamente de forma adequada, para reduzir os riscos oriundos de ameaças e perigos ambientais e de oportunidades de acesso não autorizado. Os seguintes controles devem ser considerados:

a) Os equipamentos devem ser dispostos fisicamente de forma a minimizar acessos desnecessários entre áreas de trabalho.

b) As instalações de processamento e armazenamento de informações que lidam com dados sensíveis devem ser posicionadas para reduzir o risco de as informações serem vistas casualmente durante seu uso.

c) Itens que necessitam proteção especial devem ser isolados para reduzir o nível geral de proteção exigido.

d) Controles devem ser adotados para minimizar o risco de ameaças potenciais incluindo:

   1) roubo;
   2) incêndio;
   3) explosivos;
   4) fumaça;
   5) água (ou falha no fornecimento);
   6) poeira;
   7) vibração;
   8) efeitos químicos;
   9) interferência no suprimento elétrico;
   10) radiação eletromagnética.

e) Uma organização deve considerar sua política em relação ao consumo de alimentos, bebida e cigarros nas proximidades das instalações de processamento de informações.

f) As condições ambientais devem ser monitoradas em busca de situações que possam afetar a operação das instalações de processamento de informações.

g) O uso de métodos de proteção especiais, tais como membranas para teclados, deve ser considerado para equipamentos em ambientes industriais.

h) Deve ser considerado o impacto de um desastre que aconteça nos prédios próximos, por exemplo um incêndio em um edifício vizinho, vazamento de água através do teto ou em andares abaixo do nível da rua ou uma explosão na rua.

7.2.2 Suprimento de energia

Os equipamentos devem ser protegidos contra falta de energia e outras anomalias na eletricidade. Uma fonte elétrica adequada deve ser provida de acordo com as especificações do fabricante do equipamento.

As opções para conseguir continuidade no fornecimento de energia incluem:

a) múltiplas alimentações para evitar um único ponto de falha no fornecimento de energia;

b) equipamento para suprimento de energia ininterrupto ("no-break");

c) gerador sobressalente.

Um equipamento de "no-break" para suportar um encerramento do processamento de forma ordenada ou para continuar com o processamento é recomendado para equipamentos que suportam operações críticas para o negócio. Os planos de contingência devem cobrir a ação a ser executada no caso de falha do "no-break". O equipamento de "no-break" deve ser verificado regularmente, para certificar que ele possui a capacidade adequada, e deve ser testado de acordo com as recomendações do fabricante.

Um gerador sobressalente deve ser considerado se o processamento tiver que continuar no caso de uma falta de energia prolongada. Se instalados, os geradores devem ser regularmente testados de acordo com as instruções do fabricante. Um suprimento adequado de combustível deve estar disponível para garantir que o gerador possa funcionar por um período prolongado.

Além disso, interruptores de energia de emergência devem estar localizados próximo às saídas de emergência nas salas de equipamentos, para facilitar o desligamento rápido da energia no caso de uma emergência. Iluminação de emergência deve ser provida no caso de falha na energia principal. Proteção contra raios deve ser instalada em todos os edifícios e filtros de proteção contra raios devem ser instalados em todas as linhas de comunicação externas.

7.2.3 Segurança para o cabeamento

Os cabos de energia e telecomunicação que transportam dados ou suportam serviços de informação devem ser protegidos contra interceptação ou danos. Os seguintes controles devem ser considerados:

a) Linhas de telecomunicação e energia dentro das instalações de processamento de informações devem ser subterrâneas, onde possível, ou sujeitas à proteção alternativa adequada.

b) O cabeamento de redes deve ser protegido contra interceptação não autorizada ou danos, por exemplo usando eletrodutos ou evitando-se rotas através de áreas públicas.

c) Os cabos de energia devem ser segregados dos cabos de comunicação para impedir interferência.

d) Para sistemas críticos ou sensíveis, controles adicionais devem incluir:
   1) instalação de conduto blindado e salas ou caixas trancadas nos pontos de inspeção e terminação;
   2) uso de roteamento alternativo ou mídia de transmissão alternativa;
   3) uso de cabeamento de fibra ótica;
   4) iniciação de varreduras em busca de dispositivos não autorizados que possam estar sendo conectados aos cabos.

7.2.4 Manutenção de equipamentos

Os equipamentos devem ser corretamente conservados para assegurar sua disponibilidade e integridade continuadas. Os seguintes controles devem ser considerados:

a) Os equipamentos devem passar por manutenção de acordo com os intervalos e especificações de serviço recomendados pelo fornecedor.

b) Apenas pessoal autorizado de manutenção deve executar os reparos e a manutenção nos equipamentos.

c) Devem ser mantidos registros sobre todas as falhas ocorridas ou suspeitadas e sobre todas as manutenções preventivas e corretivas.

d) Controles apropriados devem ser realizados quando se enviar equipamento para fora da organização para manutenção (ver também 7.2.6 sobre dados excluídos, apagados e sobrescritos). Todos os requisitos impostos pelas políticas de segurança devem ser obedecidos.

7.2.5 Segurança de equipamentos fora da empresa

Independentemente da propriedade, o uso de qualquer equipamento fora das instalações físicas da organização para processamento de informações deve ser autorizado pela gerência. A segurança fornecida deve ser equivalente àquela dos equipamentos *on-site* usados para o mesmo propósito, levando-se em consideração os riscos de trabalhar fora do local da organização. Equipamentos de processamento de informações incluem todas as formas de computadores pessoais, organizadores, telefones móveis, papel ou outra forma, que são mantidos para trabalho em casa ou que estão sendo transportados para longe do local de trabalho normal. As seguintes diretrizes devem ser consideradas:

a) Equipamentos e mídias retirados do prédio da organização não devem ser deixados desacompanhados em locais públicos. Em viagens, os computadores portáteis devem ser transportados como bagagem pessoal e disfarçados onde possível.

b) As instruções dos fabricantes para proteção dos equipamentos devem ser sempre observadas, por exemplo proteção contra exposição a campos eletromagnéticos intensos.

c) Os controles para trabalhos em casa devem ser determinados por uma avaliação de riscos e os controles cabíveis aplicados conforme apropriado, por

exemplo, armários-arquivos trancáveis, política de “mesa limpa” e controles de acesso aos computadores.

d) Cobertura de seguro adequada deve estar contratada para proteger equipamentos *off-site*.

Os riscos de segurança, tais como danos, roubo e “bisbilhotagem”, podem variar consideravelmente entre os locais e devem ser levados em conta na determinação dos controles mais apropriados. Mais informações sobre outros aspectos da proteção de equipamentos móveis podem ser encontrados no item 9.8.1.

7.2.6 Segurança para descarte ou reutilização de equipamentos

As informações podem ser comprometidas através do descarte ou reutilização descuidados de equipamentos (ver também 8.6.4). Dispositivos de armazenamento contendo informações sensíveis devem ser fisicamente destruídos ou regravados de forma segura em vez de se usar a função “delete” padrão.

Todos os itens de equipamento contendo mídia de armazenamento, tais como discos fixos, devem ser verificados para certificar que quaisquer dados sensíveis ou softwares licenciados foram removidos ou sobrescritos antes do descarte. Dispositivos de armazenamento danificados, que contenham dados sensíveis, podem exigir uma avaliação de riscos para determinar se tais itens devem ser destruídos, reparados ou descartados.

7.3 Controles gerais

Objetivo: Impedir o comprometimento ou roubo de informações e de facilidades de processamento de informações.

As informações e as facilidades de processamento de informações devem ser protegidas contra divulgação, modificação ou roubo por pessoas não autorizadas, e devem ser implantados controles para minimizar perdas ou danos.

Os procedimentos para manuseio e armazenamento são considerados no item 8.6.3.

7.3.1 Política de “mesa limpa” e “tela limpa”

As organizações devem considerar a adoção de uma política de “mesas limpas” para os papéis e mídia de armazenamento removível e uma política de “telas limpas” para as facilidades de processamento de informações, para reduzir os riscos de acesso não autorizado, perda de informações ou danos às informações durante e fora do horário de expediente. A política deve considerar as classificações de segurança de informação (ver 5.2), os riscos correspondentes e os aspectos culturais da organização.

Informações deixadas sobre as mesas de trabalho são passíveis de serem danificadas ou destruídas em um desastre tipo incêndio, enchente ou explosão.

Os seguintes controles devem ser considerados:

a) Onde apropriado, os papéis (relatórios) e mídia eletrônica devem ser armazenados em armários trancados adequados e/ou em outras formas de

mobiliário de segurança, quando não estiverem em uso, especialmente fora do horário do expediente.

b) Informações sensíveis ou críticas para o negócio devem ser trancadas em local separado (idealmente em um armário ou cofre à prova de fogo) quando não necessárias, especialmente quando o escritório fica vazio.

c) Computadores pessoais e terminais de computador e impressoras não devem ser deixados “logados” quando não houver um operador (usuário) junto e devem ser protegidos por *key locks*, senhas e outros controles quando não estiverem em uso.

d) Pontos de entrada e saída de correio e aparelhos de fax e telex devem ser protegidos.

e) Fotocopiadoras devem ser trancadas (ou protegidas contra uso não autorizado de alguma outra maneira) fora do horário de expediente.

f) Informações sensíveis ou confidenciais, quando impressas, devem ser retiradas da impressora imediatamente.

7.3.2 Remoção de propriedade

Equipamentos, informações ou software não devem ser retirados das instalações da organização sem autorização. Quando necessário e apropriado, os equipamentos devem ter sua saída registrada e devem ser registrados novamente quando devolvidos. Verificações aleatórias devem ser executadas para detectar remoção não autorizada de propriedade. As pessoas devem ser conscientizadas de que tais verificações aleatórias ocorrerão.

8 Gerenciamento de comunicações e operações

8.1 Procedimentos operacionais e responsabilidades

Objetivo: Garantir a operação correta e segura das facilidades de processamento de informações. As responsabilidades e os procedimentos para a gestão e operação de todas as facilidades de processamento de informações devem ser estabelecidas. Isso inclui o desenvolvimento de instruções de operação apropriadas e de procedimentos para resposta a incidentes. A segregação de tarefas (ver 8.1.4) deve ser implementada, onde apropriado, para reduzir o risco de utilização negligente ou má utilização deliberada dos sistemas.

8.1.1 Procedimentos operacionais documentados

Os procedimentos operacionais identificados pela política de segurança devem ser documentados e mantidos atualizados. Os procedimentos operacionais devem ser tratados como documentos formais e as alterações devem ser autorizadas pela gerência.

Os procedimentos devem especificar as instruções para execução detalhada de cada serviço, incluindo:

a) processamento e manuseio de informações;

b) exigências de *scheduling*, incluindo interdependências com outros sistemas, e horários mais cedo de início e mais tarde de término dos *jobs*;

c) instruções para tratamento de erros ou outras condições excepcionais, que possam surgir durante a execução do *job*, incluindo restrições no uso de utilitários do sistema (ver 9.5.5);

d) contatos de suporte na eventualidade de dificuldades operacionais ou técnicas inesperadas;

e) instruções para tratamento especial das saídas geradas, tais como o uso de papel especial ou o gerenciamento de saídas confidenciais, incluindo procedimentos para descarte seguro de saídas resultantes de *jobs* cancelados ou abortados;

f) procedimentos para reinício e recuperação, para uso no caso de falha no sistema.

Procedimentos documentados também devem ser preparados para as atividades de *housekeeping*[6] do sistema associadas com as facilidades de processamento de informações e comunicações, tais como procedimentos para iniciar e desligar o computador, *backups*, manutenção de equipamentos, gerenciamento e segurança da sala de computadores e de correio.

8.1.2 Controle das mudanças operacionais

Mudanças nas facilidades de processamento de informações e nos sistemas devem ser controladas. O controle inadequado dessas mudanças é uma causa freqüente de falhas na segurança ou nos sistemas. Responsabilidades gerenciais e procedimentos formais devem estar implantados para garantir um controle satisfatório de todas as alterações em equipamentos, softwares ou procedimentos. Os programas operacionais devem estar sujeitos a um controle estrito das alterações. Quando programas são mudados, deve ser retido um *log* para auditoria, contendo todas as informações relevantes. Alterações no ambiente operacional podem causar impacto nos aplicativos. Onde for praticável, os procedimentos para controle das mudanças operacionais e nos aplicativos deve ser integrado (ver também 10.5.1). Em especial, os seguintes controles devem ser considerados:

a) identificação e anotação de alterações significativas;

b) avaliação do impacto potencial de tais alterações;

c) procedimento formal de aprovação para alterações propostas;

d) comunicação dos detalhes das alterações para todas as pessoas relevantes;

e) procedimentos que identifiquem as responsabilidades pela interrupção e recuperação de alterações que não foram concluídas com sucesso.

---

[6] N.T.: *Housekeeping* = procedimentos que precisam ser executados para manter um computador ou sistema operando adequadamente.

8.1.3 Procedimentos para gerenciamento de incidentes

As responsabilidades e os procedimentos para gerenciamento de incidentes devem ser estabelecidos para garantir uma resposta rápida, efetiva e ordenada aos incidentes de segurança (ver também 6.3.1). Os seguintes controles devem ser considerados:

a) devem ser estabelecidos procedimentos para cobrir todos os tipos potenciais de incidente de segurança, incluindo:
   1) falhas nos sistemas de informação e perda de serviço;
   2) negação de serviço;
   3) erros resultantes de dados incompletos ou inexatos;
   4) violação de confidencialidade.

b) Além dos planos de contingência normais (projetados para recuperar sistemas ou serviços o mais rapidamente possível), os procedimentos devem cobrir também (ver também 6.3.4):
   1) análise e identificação da causa do incidente;
   2) planejamento e implementação de medidas para impedir a recorrência, se necessário;
   3) coleta de *audit trails* e provas similares;
   4) comunicação com aqueles afetados pelo incidente ou envolvidos com a recuperação dos danos provocados pelo incidente;
   5) reportar a ação à autoridade apropriada.

c) *audit trails* e provas similares devem ser recolhidas (ver 12.1.7) e guardadas em segurança, conforme apropriado, para:
   1) análise interna do problema;
   2) usar como prova relacionada a uma potencial violação de contrato, violação de exigências regulatórias ou no caso de processos civis ou criminais, por exemplo sob a legislação de proteção de dados ou mal uso de computadores;
   3) negociação de indenização por fornecedores de software e serviços.

d) Ação para recuperar de violações de segurança e corrigir falhas no sistema devem ser controladas de maneira formal e cuidadosa. Os procedimentos devem assegurar que:
   1) apenas pessoas claramente identificadas e autorizadas tenham seu acesso permitido aos sistemas e dados “reais” (ver também 4.2.2 para acesso de terceiros);
   2) todas as ações de emergência executadas sejam documentadas em detalhe;
   3) a ação de emergência seja reportada à gerência e revisada de maneira ordenada;
   4) a integridade dos controles e sistemas do negócio seja confirmada no menor tempo possível.

8.1.4 Segregação de tarefas

A segregação de tarefas é um método de reduzir o risco de má utilização acidental ou deliberada do sistema. Deve-se considerar a separação da gestão ou da execução de

determinadas tarefas ou áreas de responsabilidade, para reduzir as oportunidades de modificação não autorizada ou utilização indevida das informações ou serviços.

As organizações pequenas podem achar difícil implantar esse método de controle, mas o princípio deve ser aplicado tanto quanto for possível e praticável. Sempre que for difícil segregar, outros controles como monitoramento de atividades, *audit trails* e supervisão gerencial devem ser considerados. É importante que a auditoria da segurança permaneça independente.

Deve-se tomar cuidado para que uma pessoa sozinha não possa executar fraudes sem ser detectada nas áreas onde a responsabilidade é apenas dela. O início de um evento deve ser separado de sua autorização. Os seguintes controles devem ser considerados:

a) É importante segregar atividades que requerem conivência para serem defraudadas, como abrir uma ordem de compra e confirmar que os bens foram recebidos.

b) Se houver perigo de conivência, então os controles devem ser planejados de modo que duas ou mais pessoas sejam envolvidas, diminuindo assim a possibilidade de conspiração.

8.1.5 Separação das facilidades de desenvolvimento e de produção

Separar as facilidades de desenvolvimento, testes e produção é importante para se obter a segregação dos papéis envolvidos. As regras para transferência de software do desenvolvimento para o status operacional devem ser definidas e documentadas.

As atividades de desenvolvimento e testes podem causar sérios problemas, tais como modificação indesejada de arquivos ou do ambiente de desenvolvimento, ou falha no sistema. Deve ser considerado o nível de separação que é necessário, entre ambientes de produção, testes e desenvolvimento, para impedir problemas operacionais. Uma separação similar também deve ser implementada entre as funções de desenvolvimento e teste. Neste caso, existe uma necessidade de se manter um ambiente estável e conhecido, no qual se possa executar testes significativos, e de impedir o acesso inadequado pelo desenvolvedor.

Onde as equipes de desenvolvimento e testes tiverem acesso ao sistema operacional e a suas informações, eles podem ser capazes de introduzir código não autorizado e não testado ou alterar dados operacionais. Em alguns sistemas, essa capacidade pode ser usada impropriamente para cometer fraudes ou introduzir código malicioso ou não testado. Código malicioso ou não testado pode causar sérios problemas operacionais. Os desenvolvedores e testadores também representam uma ameaça à confidencialidade das informações operacionais.

As atividades de desenvolvimento e de testes podem causar alterações não intencionadas ao software e às informações se elas compartilharem o mesmo ambiente computacional. Separar as instalações de desenvolvimento, teste e produção é portanto desejável para reduzir o risco de alteração acidental ou acesso não autorizado para software operacional e dados do negócio. Os seguintes controles devem ser considerados:

a) Software de desenvolvimento e software operacional devem, onde possível, ser executados em processadores diferentes ou em diferentes domínios ou diretórios.

b) As atividades de desenvolvimento e testes devem ser o mais separadas possível.

c) Compiladores, editores e outros utilitários do sistema não devem ser acessíveis a partir do sistema operacional, quando não requeridos.

d) Procedimentos diferentes de *logon* devem ser usados para sistemas de produção e de testes, para reduzir o risco de erro. Os usuários devem ser encorajados a usar diferentes senhas para esses sistemas, e os menus devem exibir mensagens de identificação apropriadas.

e) A equipe de desenvolvimento deve ter acesso às senhas de produção apenas onde existem controles para emissão de senhas para o suporte dos sistemas operacionais. Os controles devem garantir que tais senhas sejam alteradas após o uso.

8.1.6 Gerenciamento de facilidades externas

A utilização de uma empresa externa contratada para gerenciar as facilidades de processamento de informações pode introduzir uma exposição potencial de segurança, tal como a possibilidade de comprometimentos, danos ou perdas de dados no *site* da contratada. Esses riscos devem ser identificados antecipadamente, e controles apropriados devem ser acordados com a empresa contratada e incorporados ao contrato (ver também 4.2.2 e 4.3 para obter orientação sobre contratos com terceiros que envolvem acesso às facilidades da organização e contratos de *outsourcing*).

Entre os aspectos particulares que devem ser tratados estão:

a) identificar aplicações sensíveis ou críticas que seria melhor manter *in-house*;

b) obter a aprovação dos proprietários internos da aplicação;

c) implicações para os planos de continuidade do negócio;

d) padrões de segurança a serem especificados, e o processo para mensurar o seu cumprimento;

e) alocação de responsabilidades e procedimentos específicos para monitorar eficazmente todas as atividades de segurança relevantes;

f) responsabilidades e procedimentos para reportar e tratar os incidentes de segurança (ver 8.1.3).

8.2 Planejamento e aceitação de sistemas

Objetivo: Minimizar os riscos de falhas nos sistemas. Planejamento antecipado e preparação são obrigatórios para assegurar a disponibilidade das capacidades e recursos adequados. Projeções das necessidades futuras de capacidade devem ser feitas, para reduzir o risco de sobrecarga no sistema. Os requisitos operacionais dos novos sistemas devem ser estabelecidos, documentados e testados antes de sua aceitação e uso.

8.2.1 Capacity planning

As demandas por recursos devem ser monitoradas e devem ser feitas projeções para o futuro para garantir que o poder de processamento e armazenamento adequados estejam disponíveis. Estas projeções devem levar em conta as necessidades de novos negócios e sistemas e as tendências atuais e estimadas no processamento de informações da organização.

Computadores *mainframe* exigem atenção especial, por causa do custo muito maior e do tempo gasto para tomar a decisão de compra de novos recursos. Os gerentes de serviços de *mainframe* devem monitorar a utilização dos recursos principais do sistema, incluindo processadores, memória principal, armazenamento de arquivos, impressoras e outros dispositivos de saída, e sistemas de comunicação. Eles devem identificar as tendências na utilização, particularmente em relação às aplicações comerciais ou ferramentas de gerenciamento de sistemas de informação.

Os gerentes devem usar essas informações para identificar e evitar gargalos potenciais que possam representar uma ameaça à segurança do sistema ou dos serviços para os usuários, e planejar a ação corretiva apropriada.

8.2.2 Aceitação de sistemas

Os critérios de aceitação para novos sistemas de informação, *upgrades* e novas versões devem ser estabelecidos e devem ser realizados testes adequados dos sistemas antes da aceitação. Os gerentes devem garantir que os requisitos e os critérios para aceitação de novos sistemas estejam claramente definidos, concordados, documentados e testados. Os seguintes controles devem ser considerados:

a) requisitos de performance e capacidade dos computadores;

b) procedimentos de reinício e recuperação de erros, e planos de contingência;

c) preparação e testes dos procedimentos operacionais de rotina segundo padrões definidos;

d) um conjunto acordado de controles de segurança em vigor;

e) procedimentos manuais eficazes;

f) arranjos para a continuidade dos negócios, conforme requerido no item 11.1;

g) evidência de que a instalação do novo sistema não afetará de maneira adversa os sistemas existentes, particularmente nos horários de pico de processamento, como fim de mês;

h) evidência de que foi considerado o efeito que o novo sistema terá sobre a segurança geral da organização;

i) treinamento na operação ou uso dos novos sistemas.

Para novos desenvolvimentos importantes, a área de produção e os usuários devem ser consultados em todos os estágios do processo de desenvolvimento para garantir a eficiência operacional do projeto do sistema proposto. Testes apropriados devem ser conduzidos para confirmar que todos os critérios de aceitação estão plenamente satisfeitos.

8.3 Proteção contra software malicioso

Objetivo: Proteger a integridade de softwares e informações.

Precauções são necessárias para impedir e detectar a introdução de softwares maliciosos. Softwares e instalações de processamento de informações são vulneráveis à introdução de software malicioso, tais como vírus de computador, “network worms”, “cavalos de Tróia” (ver também 10.5.4) e bombas lógicas. Os usuários devem ser conscientizados dos perigos relacionados com software malicioso ou não autorizado, e os gerentes devem, onde apropriado, implantar controles especiais para detectar ou impedir sua introdução. Em especial, é essencial que sejam tomadas precauções para detectar e impedir vírus em computadores pessoais.

8.3.1 Controles contra software malicioso

Devem ser implementados controles para detecção e prevenção contra softwares maliciosos e procedimentos apropriados de conscientização dos usuários. A proteção contra software malicioso deve ser baseada em conscientização sobre segurança, acesso apropriado ao sistema e controles para gerenciamento de alterações. Os seguintes controles devem ser considerados:

a) uma política formal que exija obediência às licenças de software e proíba o uso de software não autorizado (ver 12.1.2.2);

b) uma política formal para proteger contra riscos associados com a obtenção de arquivos e softwares através de redes externas, ou qualquer outro meio, indicando quais medidas de proteção devem ser tomadas (ver também 10.5, especialmente 10.5.4 e 10.5.5);

c) instalação e atualização regular de software de detecção de vírus e reparo, para varrer computadores e mídia como uma medida de precaução ou rotineiramente;

d) conduzir revisões regulares do software e dos conteúdos de dados dos sistemas que suportam processos críticos para o negócio. A presença de quaisquer arquivos não aprovados ou modificações não autorizadas deve ser formalmente investigada;

e) verificação antivírus, antes de qualquer uso, de quaisquer arquivos em mídia eletrônica de origem incerta ou não autorizada, ou arquivos recebidos de redes não confiáveis;

f) verificação contra software malicioso em quaisquer anexos de correio eletrônico e *downloads*, antes de qualquer uso. Esta verificação pode ser conduzida em locais diferentes, por exemplo em servidores de correio eletrônico, computadores *desktop* ou na entrada da rede da organização.

g) procedimentos de gerenciamento e responsabilidades para lidar com a proteção antivírus nos sistemas, treinamento sobre seu uso, como reportar e recuperar de ataques de vírus (ver 6.3 e 8.1.3);

h) planos apropriados para continuidade dos negócios para recuperar de ataques de vírus, incluindo todos os dados necessários e arranjos para *backup* e recuperação de softwares (ver tópico 11);

i) procedimentos para confirmar todas as informações relativas a software malicioso, e para garantir que os boletins de alerta sejam exatos e informativos. Os gerentes devem assegurar que sejam usadas fontes confiáveis, como publicações respeitadas, *sites* Internet confiáveis ou fornecedores de software antivírus, para diferenciar entre *hoaxes* e vírus verdadeiros. A equipe deve ser conscientizada quanto ao problema de *hoaxes* e o que fazer quando recebê-los.

Esses controles são especialmente importantes para servidores de arquivos de rede que suportam grandes quantidades de estações de trabalho.

8.4 *Housekeeping*

Objetivo: Manter a integridade e a disponibilidade dos serviços de processamento de informações e comunicações. Procedimentos de rotina devem ser implantados para executar a estratégia acordada sobre *backups* (ver 11.1), fazendo cópias *backup* de dados e treinando sua restauração em tempo hábil, registrando *log* de eventos e falhas e, onde apropriado, monitorando o ambiente computacional.

8.4.1 Backup das informações

Cópias *backup* dos softwares e das informações essenciais para o negócio devem ser executadas regularmente. Facilidades adequadas para *backup* devem ser fornecidas para assegurar que todas as informações e softwares essenciais para o negócio possam ser recuperados após um desastre ou falha em alguma mídia. Os procedimentos para *backup* de sistemas individuais devem ser regularmente testados para assegurar que eles satisfaçam os requisitos dos planos de continuidade do negócio (ver cláusula 11). Os seguintes controles devem ser considerados:

a) Um nível mínimo de informações *backup*, juntamente com registros completos e exatos das cópias *backup* e procedimentos documentados de restauração, devem ser armazenados em um local remoto, a uma distância segura para escapar de quaisquer danos no caso de um desastre no *site* principal. Pelo menos três gerações ou ciclos de informações *backup* devem ser guardados para as aplicações importantes para o negócio.

b) Informações *backup* devem ter um nível de proteção física e ambiental apropriado (ver cláusula 7) consistente com os padrões aplicados no *site* principal. Os controles aplicados à mídia no *site* principal devem ser estendidos para cobrir o *site* de guarda dos *backups*.

c) A mídia dos *backups* deve ser regularmente testada, onde praticável, para garantir que eles são confiáveis para uso emergencial quando necessário.

d) Procedimentos de restauração devem ser constantemente checados e testados para garantir que eles são eficazes e que podem ser concluídos dentro do tempo alocado nos procedimentos operacionais para recuperação.

O período de retenção para informações essenciais ao negócio e também quaisquer exigências de que cópias *archive* sejam retidas permanentemente (ver 12.1.3) devem ser determinados.

8.4.2 Logs de operador

A equipe da operação deve manter um *log* de suas atividades. Os *logs* devem incluir, conforme apropriado:

a) horários de início e fim do sistema;

b) erros no sistema e ação corretiva executada;

c) confirmação do manuseio correto de arquivos de dados e saídas geradas;

d) o nome da pessoa que fez a anotação no *log*.

Os *logs* de operador devem estar sujeitos a verificações independentes e regulares. sendo comparados com os procedimentos operacionais.

8.4.3 Log de falhas

As falhas devem ser reportadas e ações corretivas executadas. As falhas reportadas pelos usuários a respeito de problemas com o processamento de informações ou sistemas de comunicações devem ser registradas em *log*. Devem existir regras claras para tratar as falhas reportadas, incluindo:

a) revisão de *logs* de falhas para assegurar que as falhas tenham sido satisfatoriamente resolvidas;

b) revisão de medidas corretivas para assegurar que os controles não foram comprometidos e que a ação executada está totalmente autorizada.

8.5 Gerenciamento de redes

Objetivo: Assegurar a salvaguarda de informações em redes de computadores e a proteção da infra-estrutura de apoio.

O gerenciamento da segurança em redes que podem ultrapassar as fronteiras da organização exige atenção. Controles adicionais também podem ser exigidos para proteger dados sensíveis que trafegam por redes públicas.

8.5.1 Controles para redes

Diversos controles são necessários para obter e manter a segurança em redes de computadores. Os gerentes de redes devem implementar controles para garantir a segurança dos dados nas redes e a proteção de serviços que se utilizam das redes contra acesso não autorizado. Especificamente, os seguintes controles devem ser considerados:

a) A responsabilidade operacional pelas redes deve ser separada das operações de computador onde apropriado (ver 8.1.4).

b) A responsabilidades e os procedimentos para a administração de equipamento remoto, incluindo equipamento em áreas de usuários, devem ser determinados.

c) Se necessário, controles especiais devem ser estabelecidos para salvaguardar a confidencialidade e integridade dos dados que trafegam em redes públicas e

para proteger os sistemas conectados (ver 9.4 e 10.3). Controles especiais também podem ser exigidos para manter a disponibilidade dos serviços de rede e computadores conectados.

d) Atividades de gerenciamento devem ser cuidadosamente coordenadas para otimizar o serviço prestado ao negócio e para assegurar que controles estão aplicados de forma consistente em toda a infra-estrutura de processamento de informações.

8.6 Manuseio e segurança de mídia

Objetivo: Impedir danos aos ativos e interrupções nas atividades do negócio. Mídia deve ser controlada e fisicamente protegida. Procedimentos operacionais apropriados devem ser estabelecidos para proteger documentos, mídia magnética (fitas, discos, cassetes), dados de entrada/saída e documentação de sistemas contra danos, roubos e acesso não autorizado.

8.6.1 Gerenciamento de mídia removível

Devem existir procedimentos para o gerenciamento de mídias de computador removíveis, tais como fitas, discos, cassetes e relatórios impressos. Os seguintes controles devem ser considerados.

a) Se não forem mais necessários, os conteúdos existentes em qualquer mídia reutilizável que for removida da organização devem ser apagados.

b) Deve ser exigida autorização para remover qualquer mídia da organização e deve ser mantido um registro de tais remoções para guardar uma *audit trail* (ver 8.7.2).

c) Todas as mídias devem ser armazenadas em um ambiente seguro, de acordo com as especificações dos fabricantes.

Todos os procedimentos e níveis de autorização devem ser claramente documentados.

8.6.2 Descarte de mídia

Mídia deve ser descartada de maneira segura e cuidadosa quando não for mais necessária. Informações sensíveis podem vazar para pessoas estranhas à organização através de mídia descartada sem cuidados. Procedimentos formais para descarte seguro de mídia devem ser estabelecidos para minimizar este risco. Os seguintes controles devem ser considerados:

a) Mídia contendo informações sensíveis deve ser armazenada e descartada de forma cuidadosa e segura (por exemplo, por incineração ou picotagem) ou esvaziada de dados para uso por outro aplicativo dentro da organização.

b) A lista seguinte identifica os itens que podem exigir descarte seguro:

1) documentos em papel;
2) gravações de voz ou outras gravações;
3) papel carbono;
4) relatórios impressos;
5) fitas de impressora de utilização única;

6) fitas magnéticas;
7) discos ou cassetes removíveis;
8) mídia de armazenamento ótico (todas as formas, incluindo mídia usada pelos fabricantes para distribuição de software);
9) listagens de programas;
10) dados de teste;
11) documentação de sistemas.

c) Pode ser mais fácil recolher todos os itens de mídia e descartá-los de forma segura, do que tentar separar os itens sensíveis.

d) Muitas organizações oferecem serviços de coleta e descarte para papéis, equipamentos e mídia. Deve-se tomar cuidado na seleção de um fornecedor com controles adequados e experiência.

e) Descarte de itens sensíveis deve ser registrado, onde possível, para manter uma *audit trail*.

Ao se acumular mídia para descarte, deve-se considerar o efeito de agregação, que pode fazer com que uma grande quantidade de informações não confidenciais se torne mais sensível do que uma pequena quantidade de informações confidenciais.

8.6.3 Procedimentos de manuseio de informações

Procedimentos para o manuseio e armazenamento de informações devem ser estabelecidos para proteger tais informações contra divulgação não autorizada ou utilização indevida. Devem ser redigidos procedimentos para manusear informações, de forma consistente com sua classificação (ver 5.2), em documentos, sistemas de computador, redes, computação móvel, comunicação móvel, correio, correio de voz, comunicações de voz em geral, multimídia, serviços e facilidades postais, uso de aparelhos de fax e outros itens sensíveis, como cheques em branco e faturas. Os seguintes controles devem ser considerados (ver também 5.2. e 8.7.2):

a) manuseio e rotulagem de todas as mídias [ver também 8.7.2a)];

b) restrições de acesso para identificar pessoal não autorizado;

c) manutenção de um registro formal dos receptores autorizados de dados;

d) assegurar que os dados de entrada estejam completos, que o processamento seja concluído adequadamente e que seja aplicada uma validação das saídas produzidas;

e) proteção de dados gravados em *spool*, aguardando impressão, em um nível adequado com sua confidencialidade;

f) armazenamento das mídias em um ambiente que esteja de acordo com as especificações dos fabricantes;

g) manter a distribuição de dados em um nível mínimo;

h) marcação clara de todas as cópias de dados para a atenção do receptor autorizado;

i) revisão, a intervalos regulares, das listas de distribuição e listas de receptores autorizados.

8.6.4 Segurança da documentação dos sistemas

A documentação dos sistemas pode conter várias informações sensíveis, como descrições de processos de aplicativos, procedimentos, estruturas de dados e processos de autorização (ver também 9.1). Os seguintes controles devem ser considerados para proteger a documentação dos sistemas contra acesso não autorizado:

a) A documentação dos sistemas deve ser guardada de forma segura.

b) A lista de acesso à documentação de sistemas deve ser o mais reduzida possível e autorizada pelo proprietário da aplicação.

c) Documentação de sistemas mantida em uma rede pública, ou fornecida via uma rede pública, deve ser protegida adequadamente.

8.7 Intercâmbios de informações e softwares

Objetivo: Impedir perda, modificação ou uso indevido de informações intercambiadas entre organizações.

Os intercâmbios de informações e software entre organizações devem ser controlados e devem obedecer à qualquer legislação relevante (ver cláusula 12).
Os intercâmbios devem ser executados com base em contratos. Procedimentos e padrões para proteger informações e mídias em trânsito devem ser estabelecidos. Devem ser consideradas as implicações para o negócio e para a segurança associadas com intercâmbio eletrônico de dados, comércio eletrônico e correio eletrônico e os controles necessários.

8.7.1 Contratos para intercâmbio de informações e softwares

Contratos, alguns dos quais podem ser formais, incluindo contratos para custódia de software quando apropriado, devem ser estabelecidos para o intercâmbio (seja eletrônico ou manual) de informações e softwares entre organizações. O conteúdo relativo às questões de segurança de tais contratos deve refletir a confidencialidade das informações comerciais envolvidas. Os contratos sobre condições de segurança devem considerar:

a) responsabilidades gerenciais para controlar e notificar transmissão, expedição e recepção;

b) procedimentos para notificar o remetente, transmissão, expedição e recepção;

c) padrões técnicos mínimos para embalagem e transmissão;

d) padrões de identificação de/para *courier*;

e) responsabilidades, inclusive financeiras, no caso de perda de dados;

f) uso de um sistema de rotulagem acordado entre as partes para as informações críticas ou sensíveis, garantindo que o significado do rótulo seja entendido imediatamente e que as informações sejam protegidas adequadamente;

g) propriedade das informações e software e responsabilidades pela proteção de dados, respeito aos *copyrights* dos softwares e considerações similares (ver 12.1.2 e 12.1.4);

h) padrões técnicos para ler e gravar informações e softwares;

i) quaisquer controles especiais que possam ser necessários para proteger itens sensíveis, tais como chaves de criptografia (ver 10.3.5).

8.7.2 Segurança de mídia em trânsito

Informações podem ser vulneráveis a acesso não autorizado, uso indevido ou corrompimento durante transporte físico, por exemplo ao se enviar mídia por meio dos correios ou de serviço de *courier*. Os seguintes controles devem ser aplicados para salvaguardar mídia de computador que é transportada entre locais diferentes:

a) Devem ser usados *couriers* ou transportadoras confiáveis. No contrato deve ser acordada com a gerência uma lista de *couriers* autorizados e deve ser implementado um procedimento para confirmar a identificação dos *couriers*.

b) A embalagem deve ser suficiente para proteger os conteúdos contra quaisquer danos físicos que possam ocorrer durante o trânsito e deve estar de acordo com as especificações dos fabricantes.

c) Controles especiais devem ser adotados, onde necessário, para proteger informações sensíveis contra divulgação não autorizada ou modificação. Exemplos incluem:

   1) uso de contêineres trancados;
   2) entrega pessoal;
   3) embalagem que evidencie violação (que revele qualquer tentativa de obter acesso);
   4) em casos excepcionais, o desmembramento do material em mais de uma entrega e o envio por mais de uma rota;
   5) uso de assinaturas digitais e criptografia (ver 10.3).

8.7.3 Segurança para comércio eletrônico

O comércio eletrônico pode envolver o uso de intercâmbio de dados eletrônicos (EDI), correio eletrônico e transações *online* através de redes públicas, tais como a Internet. O comércio eletrônico é vulnerável a muitas ameaças pela rede, que podem resultar em atividade fraudulenta, disputa contratual e divulgação ou modificação de informações. Devem ser aplicados controles para proteger o comércio eletrônico contra tais ameaças. As considerações de segurança para o comércio eletrônico incluem os seguintes controles:

a) Autenticação. Qual nível de segurança deve o cliente e o negociante exigirem quanto à identidade alegada de cada um?

b) Autorização. Quem está autorizado a definir preços, emitir ou assinar documentos comerciais importantes? Como o parceiro comercial sabe disto?

c) Processos relacionados com contratos e propostas. Quais são os requisitos de confidencialidade, integridade e prova de envio e recepção de documentos importantes e da não repudiação de contratos?

d) Informações de preços. Qual o nível de confiança que pode ser depositado na integridade da lista de preços anunciada e na confidencialidade de acordos confidenciais para descontos?

e) Transações de encomendas. Como é fornecida a confidencialidade e integridade para detalhes de manipulação de encomendas, pagamentos, entrega e confirmação de recebimento?

f) Escrutínio. Qual grau de detalhamento no exame é apropriado para checar informações de pagamento fornecidas pelo cliente?

g) Quitação. Qual é a forma de pagamento mais apropriada para resguardar contra fraudes?

h) Encomendas. Qual proteção é necessária para manter a confidencialidade e integridade das informações de encomenda, e para evitar a perda ou duplicidade de transações?

i) Responsabilidade financeira. Quem arca com o risco de transações fraudulentas?

Muitas das considerações acima podem ser tratadas com a aplicação de técnicas de criptografia esboçadas no item 10.3, levando em conta a obediência às exigências legais (ver 12.2, especialmente 12.1.6 sobre legislação de criptografia).

Os acordos de comércio eletrônico entre parceiros comerciais devem ser apoiados por um contrato documentado que compromete ambas as partes com os termos acordados do intercâmbio, incluindo detalhes sobre autorização [ver item b) acima]. Outros contratos com provedores de serviços de informação e de redes de valor agregado podem ser necessários.

Sistemas de comércio públicos devem divulgar seus termos de negócio para os clientes.

Deve-se levar em consideração a resiliência a ataques do *host* usado para comércio eletrônico, e as implicações de segurança de qualquer interconexão de redes exigida para sua implementação (ver 9.4.7).

8.7.4 Segurança para correio eletrônico

8.7.4.1 *Riscos de segurança*

O correio eletrônico vem sendo usado para comunicações comerciais, substituindo as formas tradicionais de comunicação tais como telex e cartas. O correio eletrônico difere das formas tradicionais de comunicação comercial, por exemplo, pela sua velocidade, estrutura de mensagens, grau de informalidade e vulnerabilidade a ações não autorizadas. Deve-se levar em consideração a necessidade de controles para reduzir os riscos de segurança criados pelo correio eletrônico. Os riscos de segurança incluem:

a) vulnerabilidade das mensagens a acesso não autorizado ou modificação ou negação de serviço;

b) vulnerabilidade a erros, como endereçamento incorreto ou mal direcionamento, e a confiabilidade e disponibilidade gerais do serviço;

c) impacto, nos processos do negócio, de uma mudança na mídia de comunicação; por exemplo, o efeito do aumento da velocidade da expedição ou o efeito de enviar mensagens formais de pessoa para pessoa em vez de empresa para empresa;

d) considerações legais, tais como a necessidade potencial de prova de origem, expedição, entrega e aceitação;

e) implicações de publicar listas de pessoal acessíveis externamente;

f) controlar acesso de usuários remotos a contas de correio eletrônico.

8.7.4.2 *Política sobre correio eletrônico*

As organizações devem estabelecer uma política clara relativa ao uso de correio eletrônico, incluindo:

a) ataques ao correio eletrônico, como vírus e interceptação;

b) proteção dos anexos nas mensagens eletrônicas;

c) diretrizes sobre quando não usar correio eletrônico;

d) responsabilidade dos empregados em não comprometer a empresa; por exemplo, envio de mensagens eletrônicas difamatórias, utilização para assédio, compras não autorizadas;

e) uso de técnicas criptográficas para proteger a confidencialidade e a integridade das mensagens eletrônicas (ver 10.3);

f) retenção de mensagens que, se armazenadas, podem ser descobertas em casos de litígios;

g) controles adicionais para examinar cuidadosamente mensagens que não podem ser autenticadas.

8.7.5 Segurança de sistemas de automação de escritórios

Políticas e diretrizes devem ser preparadas e implementadas para controlar os riscos para a segurança e para o negócio associados com sistemas de automação de escritórios. Estes propiciam oportunidades para disseminação e compartilhamento mais rápidos de informações comerciais usando uma combinação de: documentos, computadores, computação móvel, comunicações móveis, correio, correio de voz, comunicações verbais em geral, multimídia, serviços/facilidades postais e equipamentos de fax.

Os cuidados tomados em relação às implicações de segurança decorrentes da interconexão de tais facilidades devem incluir:

a) vulnerabilidades das informações nos sistemas de automação de escritórios, tal como gravação de telefonemas ou conferências telefônicas, confidencialidade de telefonemas, armazenagem de faxes, abertura de correspondência, distribuição de correspondência;

b) política e controles apropriados para gerenciar o compartilhamento de informações, por exemplo o uso de *bulletin boards* eletrônicos corporativos (ver 9.1);

c) excluir categorias de informações sensíveis do negócio se o sistema não fornecer um nível adequado de proteção (ver 5.2);
d) restringir o acesso a informações de agenda relativas a indivíduos selecionados, tais como a equipe que trabalha em projetos sensíveis;
e) a adequabilidade do sistema para suportar aplicações administrativas, tais como comunicar ordens ou autorizações;
f) categorias de pessoal, contratados ou parceiros comerciais autorizados a usar o sistema e os locais de onde ele pode ser acessado (ver 4.2);
g) restringir facilidades selecionadas a categorias específicas de usuários;
h) identificar o status dos usuários, por exemplo empregados da organização ou prestadores de serviço em listas para o benefício de outros usuários;
i) retenção e *backup* das informações mantidas no sistema (ver 12.1.3 e 8.4.1);
j) requisitos e providências para *fallback* (ver 11.1).

8.7.6 Sistemas disponibilizados publicamente

Devem ser tomados cuidados para proteger a integridade de informações publicadas eletronicamente para impedir modificação não autorizada, que poderia prejudicar a reputação da organização publicadora. As informações em um sistema disponibilizado publicamente, tal como informações em um servidor de Web acessíveis via Internet, podem necessitar obedecer a leis, normas e regulamentos na jurisdição onde o sistema está localizado ou onde os negócios ocorrem. Deveria existir um processo formal de autorização antes que as informações sejam disponibilizadas publicamente.

Software, dados e outras informações que necessitem de um alto nível de integridade, tornadas disponíveis em um sistema público, devem ser protegidas pelos mecanismos apropriados, como assinaturas digitais (ver 10.3.3). Sistemas de publicação eletrônica, especialmente aqueles que permitem *feedback* e entrada direta de informações, devem ser cuidadosamente controlados de forma que:

a) as informações sejam obtidas de acordo com qualquer legislação de proteção de dados existente (ver 12.1.4);
b) as informações introduzidas no sistema de publicação e processadas por ele sejam processadas inteiramente e com exatidão em tempo adequado;
c) as informações sensíveis sejam protegidas durante o processo de coleta e quando armazenadas;
d) o acesso ao sistema de publicação não permita o acesso não intencionado a redes em que esteja conectado.

8.7.7 Outras formas de intercâmbio de informações

Procedimentos e controles devem estar implantados para proteger o intercâmbio de informações através do uso de facilidades de voz, fac-símile e vídeo-comunicações. As informações podem ser comprometidas devido à falta de conscientização, política ou procedimentos sobre o uso de tais facilidades, como por exemplo, conversas ouvidas por acaso em telefone móvel em local público, gravações em secretárias

eletrônicas ouvidas por acaso, acesso não autorizado a sistemas discados de correio de voz ou enviar faxes acidentalmente para a pessoa errada.

As operações da organização podem ser perturbadas e as informações podem ser comprometidas se as facilidades de comunicação apresentarem falhas, ficarem sobrecarregadas ou forem interrompidas (ver 7.2 e cláusula 11). As informações também podem ser comprometidas se forem acessadas por usuários não autorizados (ver cláusula 9).

Deve ser estabelecida uma declaração clara da política com os procedimentos que se espera que os empregados sigam no uso de comunicações de voz, fax e vídeo. Ela deve incluir:

a) lembrar aos funcionários que eles devem tomar as precauções apropriadas, tais como não revelar informações sensíveis, de modo a evitar serem ouvidos por acaso ou interceptados ao fazerem telefonemas por:
   1) pessoas nas imediações, particularmente ao usar telefones móveis;
   2) escuta telefônica e outras formas de espionagem através de acesso físico ao aparelho telefônico ou à linha telefônica, ou através de receptores de varredura quando se usar telefones móveis analógicos;
   3) pessoas que estejam ao lado de quem recebe o telefonema.
b) lembrar aos funcionários que eles não devem manter conversas confidenciais em áreas públicas ou escritórios abertos e salas de reunião com paredes finas;
c) não deixar mensagens em secretárias eletrônicas, já que elas podem ser ouvidas por pessoas não autorizadas, armazenadas em sistemas de uso comum ou armazenadas incorretamente como um resultado de rediscagem;
d) lembrar aos funcionários sobre os problemas relacionados com o uso de equipamentos de fax, a saber:
   1) acesso não autorizado a memórias internas de mensagens para buscar mensagens;
   2) programação deliberada ou acidental de máquinas para enviar mensagens para números específicos;
   3) enviar documentos ou imagens para o número errado, ou discando o número errado ou usando um número armazenado errado.

9 Controle de Acesso

9.1 Necessidades de controle de acesso

Objetivo: Controlar o acesso às informações. O acesso a informações e processos do negócio deve ser controlado com base nas necessidades de segurança e do negócio. Deve-se levar em conta as políticas para disseminação e autorização das informações.

9.1.1 Política de controle de acesso

9.1.1.1 *Política e requisitos do negócio*

Os requisitos de controle de acesso na organização devem ser definidos e documentados. As regras e direitos de controle de acesso para cada usuário ou grupo de usuários devem ser claramente definidas em uma declaração de política de acesso. Os usuários e os provedores de serviços devem receber uma declaração clara dos requisitos a serem satisfeitos pelos controles de acesso.

A política deve considerar o seguinte:

a) requisitos de segurança das aplicações individuais do negócio;
b) identificação de todas as informações relacionadas às aplicações do negócio;
c) políticas para disseminação e autorização de informações, como o princípio do “saber apenas quando necessário” e níveis de segurança e classificação de informações;
d) consistência entre o controle de acesso e as políticas de classificação de informação dos diferentes sistemas e redes;
e) legislação relevante e quaisquer obrigações contratuais relacionadas com a proteção de acesso para dados ou serviços (ver cláusula 12);
f) padronização de perfis de usuário para categorias comuns de serviço;
g) gerenciamento de direitos de acesso em um ambiente de rede e distribuído que reconhece todos os tipos de conexão disponíveis.

9.1.1.2 *Regras para controle de acesso*

Na especificação das regras para controle de acesso, é preciso considerar com cuidado o seguinte:

a) diferenciar entre regras que devem ser sempre obedecidas e regras que são opcionais ou condicionais;
b) estabelecer regras baseadas na premissa “O que deve ser geralmente proibido a menos que seja expressamente permitido” em vez de usar a regra mais fraca “Tudo é geralmente permitido a menos que seja expressamente proibido”;
c) mudanças nos rótulos das informações (ver 5.2) que são iniciadas automaticamente pelas facilidades de processamento de informação e aquelas iniciadas à discrição de um usuário;
d) mudanças nas permissões de usuários que são iniciadas automaticamente pelo sistema de informações e aquelas iniciadas por um administrador;
e) regras que exigem a aprovação do administrador ou outra aprovação antes de sua decretação e aquelas que não exigem.

9.2 Gerenciamento do acesso de usuários

Objetivo: Impedir acesso não autorizado aos sistemas de informação.

Procedimentos formais devem ser implantados para controlar a alocação de direitos de acesso a sistemas e serviços de informação.
Os procedimentos devem cobrir todos os estágios do ciclo de vida do acesso dos usuários, desde o cadastramento inicial de novos usuários até a retirada final de usuários que não mais necessitam de acesso aos sistemas e serviços de informação.

Atenção adequada deve ser dada, onde apropriado, à necessidade de controlar a alocação de direitos privilegiados de acesso, que permitem aos usuários sobrepujar os controles do sistema.

9.2.1 Cadastramento de usuários

Deve existir um procedimento formal de cadastramento e descadastramento de usuários para a concessão de acesso a todos os sistemas e serviços de informação multiusuários.

O acesso a serviços de informação multiusuários deve ser controlado através de um processo formal de cadastramento de usuários, que deve incluir:

a) usar IDs de usuário exclusivas, de modo que os usuários possam ser relacionados com suas ações e responsabilizados por elas. O uso de IDs de grupo deve ser permitido apenas onde elas sejam adequadas para o trabalho executado;

b) confirmar que o usuário tem autorização do proprietário do sistema para o uso do sistema ou serviço de informação. Aprovação separada para os direitos de acesso pela gerência também pode ser conveniente;

c) confirmar que o nível de acesso concedido é apropriado para os fins do negócio (ver 9.1.) e consistente com a política de segurança da organização; por exemplo, não compromete a segregação de tarefas (ver 8.14);

d) entregar aos usuários um documento escrito com seus direitos de acesso;

e) exigir que os usuários assinem declarações indicando que eles entendem as condições de acesso;

f) assegurar que os provedores de serviço não concedam acesso até os procedimentos de autorização terem sido concluídos;

g) manter um registro formal de todas as pessoas cadastradas para usar o serviço;

h) remover imediatamente os direitos de acesso de usuários que trocaram de função ou deixaram a organização;

i) verificar periodicamente e remover IDs de usuários e contas redundantes;

j) assegurar que IDs de usuário redundantes não sejam emitidas para outros usuários.

Deve ser dada atenção à inclusão de cláusulas nos contratos de trabalho e contratos de serviços que especifiquem sanções no caso de tentativas de acesso não autorizado pelos empregados ou pessoas contratadas (ver também 6.1.4 e 6.3.5).

9.2.2 Gerenciamento de privilégios

A alocação e o uso de privilégios (qualquer recurso ou facilidade de um sistema de informações multiusuário que permite ao usuário sobrepujar os controles do sistema ou aplicativo) devem ser restritos e controlados. O uso inapropriado de privilégios de sistema freqüentemente é um dos principais fatores contribuintes para a falha de sistemas que foram violados.

Sistemas multiusuários que exigem proteção contra acesso não autorizado devem ter a alocação de privilégios controlada através de procedimento formal de autorização. Os seguintes passos devem ser considerados:

a) Devem ser identificados os privilégios associados com cada produto de sistema, por exemplo sistema operacional, sistema de gerenciamento de banco de dados e cada aplicativo, e as categorias de pessoal para as quais eles precisam ser alocados.

b) Os privilégios devem ser alocados para os indivíduos na base da necessidade de uso e na base de evento por evento, isto é, o requisito mínimo para seu papel funcional apenas quando necessário.

c) Um processo de autorização e um registro de todos os privilégios alocados devem ser mantidos. Os privilégios não devem ser concedidos até que o processo de autorização esteja concluído.

d) O desenvolvimento e o uso de rotinas do sistema deve ser promovido para evitar a necessidade de conceder privilégios a usuários.

e) Os privilégios devem ser concedidos para uma identificação de usuário diferente daquelas empregadas para uso normal do negócio.

9.2.3 Gerenciamento de senhas de usuário

As senhas são um meio comum de validar a identidade de um usuário para acessar um sistema ou serviço de informações. A alocação de senhas deve ser controlada através de um processo administrativo formal, cujo enfoque deveria ser:

a) exigir que os usuários assinem uma declaração de manter confidencial as senhas pessoais e de manter as senhas de grupos somente entre as pessoas do grupo (isto poderia ser incluído nos termos e condições do contrato de trabalho, ver 6.1.4);

b) garantir, onde os usuários forem responsáveis por manter suas próprias senhas, que eles sejam providos inicialmente com uma senha temporária segura a qual eles sejam forçados a alterar imediatamente. As senhas temporárias fornecidas quando um usuário esquece sua senha devem ser fornecidas apenas após identificação positiva do usuário;

c) exigir que as senhas temporárias sejam dadas aos usuários de uma maneira segura. O uso de mensagens de correio eletrônico de terceiros ou desprotegidas (texto simples) deve ser evitado. Os usuários devem acusar o recebimento das senhas.

As senhas nunca devem ser guardadas em um sistema de computador sob forma desprotegida.

Outras tecnologias para identificação e autenticação de usuários, tais como biométrica (verificação de impressão digital), verificação de assinatura e uso de peças de hardware, tais como cartões com *chip*, estão disponíveis e devem ser consideradas se apropriado.

9.2.4 Revisão dos direitos de acesso dos usuários

Para manter controle efetivo sobre o acesso aos serviços de informações, a gerência deve conduzir um processo formal, a intervalos regulares, para revisar os direitos de acesso dos usuários de forma que:

a) os direitos de acesso dos usuários sejam revisados a intervalos regulares (um período de 6 meses é recomendado) e após quaisquer alterações (ver 9.2.1)

b) as autorizações para direitos privilegiados de acesso (ver 9.2.2) devem ser revisadas a intervalos mais freqüentes; é recomendado um período de 3 meses;

c) a alocação de privilégios seja verificada em intervalos regulares para garantir que não sejam obtidos privilégios não autorizados.

9.3 Responsabilidades dos usuários

Objetivo: Impedir acesso de usuários não autorizados. A cooperação dos usuários autorizados é essencial para a eficácia da segurança. Os usuários devem ser conscientizados de suas responsabilidades quanto à manutenção de controles eficazes de acesso, particularmente o uso de senhas e a segurança do equipamento do usuário.

9.3.1 Uso de senhas

Os usuários devem seguir as boas normas de segurança na seleção e uso de senhas.

As senhas fornecem um meio de validar a identidade do usuário e assim estabelecer direitos de acesso aos serviços ou facilidades de processamento de informações. Todos os usuários devem ser aconselhados a:

a) manter confidenciais as senhas;

b) evitar manter anotação das senhas em papel, a menos que possam ser guardadas com segurança;

c) alterar senhas sempre que houver qualquer indicação de possível comprometimento da senha ou do sistema;

d) selecionar senhas de qualidade com um tamanho mínimo de seis caracteres, que:

   1) sejam fáceis de lembrar;
   2) não sejam baseadas em algo que alguém poderia facilmente deduzir e obter usando informações relacionadas com a pessoa, por exemplo, nomes, números de telefones, datas de nascimento, etc.;
   3) sejam isentas de caracteres consecutivos idênticos ou grupos totalmente numéricos ou totalmente alfabéticos.

e) alterar senhas a intervalos regulares ou baseado na quantidade de acessos (senhas para contas privilegiadas devem ser alteradas com mais freqüência do que as senhas normais), e evitar reutilizar ou usar ciclicamente senhas antigas;

f) alterar senhas temporárias no primeiro *logon* ;

g) não incluir senhas em qualquer processo automático de *logon*, por exemplo armazenadas em uma macro ou tecla de função;

h) não compartilhar senhas individuais.

Se os usuários precisarem acessar múltiplos serviços ou plataformas e forem obrigados a manter múltiplas senhas, eles devem ser avisados de que podem usar uma única senha de qualidade [ver item d) acima] para todos os serviços que possuam um nível razoável de proteção para senhas armazenadas.

9.3.2 Equipamentos de usuário desassistidos

Os usuários devem se assegurar de que equipamentos desassistidos possuem proteção apropriada. Os equipamentos instalados nas áreas dos usuários, como estações de trabalho ou servidores de arquivos, podem exigir proteção específica contra acesso não autorizado quando deixados desassistidos por um período prolongado. Todos os usuários e contratados devem ser conscientizados dos requisitos e procedimentos de segurança para proteger equipamento desassistido, bem como de suas responsabilidades para implementação de tal proteção. Os usuários devem ser aconselhados a:

a) encerrar sessões ativas quando terminarem, a menos que elas possam ser protegidas por um mecanismo de tranca, como um protetor de tela com senha;

b) desligar *(logoff)* os computadores *mainframe* quando a sessão estiver finalizada (isto é, não apenas desligar o terminal ou o PC);

c) proteger PCs ou terminais contra uso não autorizado por meio de um *key lock* ou um controle equivalente, como acesso por senha, quando não estiverem em uso.

9.4 Controle de acesso à rede

Objetivo: Proteção de serviços que utilizam redes.

O acesso a serviços em redes internas e externas deve ser controlado.

Isto é necessário para assegurar que os usuários que têm acesso a redes e serviços em rede não comprometam a segurança de tais serviços, usando-se:

a) interfaces apropriadas entre a rede da organização e as redes de propriedade de outras organizações ou redes públicas;

b) mecanismos apropriados para autenticação de usuários e equipamentos;

c) controle do acesso dos usuários aos serviços de informações.

9.4.1 Política sobre o uso de serviços em rede

Conexões inseguras com serviços em rede podem afetar toda a organização. Os usuários devem ter acesso direto apenas aos serviços que eles foram especificamente autorizados a usar. Este controle é particularmente importante para conexões de rede com aplicações sensíveis ou críticas ou para usuários em locais de alto risco, como áreas públicas ou externas que estão fora da gestão e controle de segurança da organização.

Deve ser formulada uma política relacionada ao uso de redes e de serviços em rede. Ela deve cobrir:

a) as redes e os serviços em rede cujo acesso é permitido;

b) procedimentos de autorização para determinar quem está autorizado a acessar quais redes e serviços em rede;

c) controles e procedimentos administrativos para proteger o acesso a conexões de rede e serviços em rede.

Esta política deve ser consistente com a política de controle de acesso da organização (ver 9.1).

9.4.2 Path obrigatório

O *path* do terminal do usuário até o serviço informatizado pode precisar ser controlado. As redes são projetadas para permitir máximo escopo no compartilhamento de recursos e flexibilidade de roteamento. Esses recursos também podem propiciar oportunidades para acesso não autorizado a aplicações da organização ou uso não autorizado das facilidades de informação. Incorporar controles que restrinjam a rota entre o terminal do usuário e os serviços informatizados que o usuário está autorizado a acessar, como por exemplo criando um *path* obrigatório, pode reduzir tais riscos.

O objetivo de um *path* obrigatório é impedir quaisquer usuários de selecionar rotas que estão fora da rota entre o terminal do usuário e os serviços que o usuário está autorizado a acessar.

Isto geralmente requer a implementação de diversos controles em diferentes pontos na rota. O princípio é limitar as opções de roteamento em cada ponto na rede, através de escolhas predefinidas.

São exemplos disto:

a) alocar linhas ou números de telefones dedicados;

b) conectar portas automaticamente com sistemas aplicativos ou *gateways* de segurança especificados;

c) limitar as opções de menus e submenus para usuários individuais;

d) impedir *roaming* de rede ilimitado;

e) para usuários externos da rede, obrigar o uso de sistemas aplicativos e/ou *gateways* de segurança especificados;

f) controlar ativamente as comunicações permitidas entre origem e destino via *gateways* de segurança, como *firewalls*;

g) restringir o acesso à rede através da implantação de domínios lógicos separados, como redes virtuais privadas, para grupos de usuários dentro da organização (ver também 9.4.6).

Os requisitos para um *path* obrigatório devem ser baseados na política de controle de acesso do negócio (ver 9.1.).

9.4.3 Autenticação de usuário para conexões externas

Conexões externas apresentam um potencial para acesso não autorizado às informações do negócio, como por exemplo acesso através de métodos *dial-up*. Portanto, o acesso de usuários remotos deve estar sujeito à autenticação. Existem tipos diferentes de métodos de autenticação e alguns fornecem um nível de proteção maior do que outros, tais como métodos baseados no uso de técnicas criptográficas, que podem propiciar uma autenticação mais poderosa. É importante determinar o nível de proteção requerida a partir de uma avaliação de riscos. Isto é necessário para a seleção apropriada de um método de autenticação.

Autenticação de usuários remotos pode ser conseguida usando-se, por exemplo, uma técnica baseada em criptografia, *tokens* de hardware ou protocolo tipo “challenge/response”. Linhas privadas dedicadas ou uma funcionalidade para checar endereços de usuário na rede também podem ser usadas para fornecer garantia da origem das conexões.

Procedimentos e controles para *dial-back*, por exemplo usando modems *dial-back*, podem fornecer proteção contra conexões não autorizadas ou indesejadas às facilidades de processamento de informações de uma organização. Este tipo de controle autentica os usuários que tentam estabelecer uma conexão a uma rede da organização a partir de locais remotos. Quando usar este controle, uma organização não deve usar serviços de rede que incluem encaminhamento de chamadas ou, se eles incluírem, deve desabilitar o uso de tais recursos para evitar vulnerabilidades associadas com encaminhamento de chamadas. Também é importante que o processo de *call-back* inclua confirmação de que realmente ocorreu uma desconexão na ponta da organização. Caso contrário, o usuário remoto pode reter a linha aberta fingindo que ocorreu uma confirmação de *call-back*. Procedimentos e controles de *call-back* devem ser cuidadosamente testados quanto a esta possibilidade.

9.4.4 Autenticação de nodo

Um recurso para conexão automática com um computador remoto pode fornecer um meio para obter acesso não autorizado a uma aplicação da organização. Conexões com sistemas de computadores remotos devem portanto ser autenticadas. Isto é especialmente importante se a conexão usar uma rede que está fora do controle do gerenciamento de segurança da organização. Alguns exemplos de autenticação e de como ela pode ser obtida são citados no item 9.3.4 acima.

Autenticação de nodos pode servir como um meio alternativo de autenticar grupos de usuários remotos onde eles estejam conectados com uma instalação de computadores compartilhada e segura (ver 9.4.3).

9.4.5 Proteção de porta de diagnóstico remoto

Acesso a portas de diagnóstico deve ser controlado de forma segura. Muitos computadores e sistemas de comunicação são instalados com um recurso de diagnóstico remoto por linha discada para uso pelos engenheiros de manutenção. Se desprotegidas, estas portas de diagnóstico propiciam um meio para acesso não autorizado. Portanto, elas devem ser protegidas por um mecanismo de segurança adequado, como um *key lock*, e um procedimento para garantir que elas sejam

acessíveis apenas através de combinação entre o gerente do serviço de computador e o pessoal de suporte de hardware/software que solicitar o acesso.

9.4.6 Segregação em redes

As redes estão cada vez mais se estendendo além das fronteiras tradicionais das organizações, à medida que são formadas parcerias comerciais que podem necessitar de interconexão ou compartilhamento de facilidades de processamento de informações e redes. Tais extensões podem aumentar o risco de acesso não autorizado aos sistemas de informação que já usam a rede, alguns dos quais podem exigir proteção contra outros usuários da rede devido à sua confidencialidade ou criticalidade. Em tais circunstâncias, a introdução de controles dentro da rede, para segregar grupos de serviços de informação, usuários e sistemas de informação, deve ser considerada.

Um método de controlar a segurança de grandes redes é dividi-las em domínios lógicos separados, como domínios das redes internas da organização e domínios das redes externas, cada um protegido por um perímetro de segurança definido. Um tal perímetro pode ser implementado pela instalação de um *gateway* seguro entre as duas redes a serem interconectadas para controlar o acesso e o fluxo de informações entre os dois domínios. Este *gateway* deve ser configurado para filtrar o tráfego entre esses domínios (ver 9.4.7 e 9.4.8) e para bloquear acessos não autorizados, de acordo com a política de controle de acesso da organização (ver 9.1). Um exemplo deste tipo de *gateway* é aquele comumente referido como *firewall*.

Os critérios para segregação de redes em domínios devem ser baseados na política de controle de acesso e nos requisitos de acesso (ver 9.1) e também levar em conta o custo relativo e o impacto na performance de incorporar tecnologia adequada para roteamento de rede ou *gateway* (ver 9.4.7 e 9.4.8).

9.4.7 Controle das conexões de rede

Os requisitos da política de controle de acesso para redes compartilhadas, especialmente aquelas que se estendem além das fronteiras da organização, podem exigir a incorporação de controles para restringir a capacidade de conexão dos usuários. Tais controles podem ser implementados através de *gateways* para a rede que filtram o tráfego utilizando tabelas ou regras predefinidas. As restrições aplicadas devem ser baseadas na política de acesso e nos requisitos das aplicações do negócio (ver 9.1) e devem ser mantidas e atualizadas de acordo.

São exemplos de aplicações às quais restrições deveriam ser aplicadas:

a) correio eletrônico;

b) transferência de arquivo *one-way* (em um único sentido)

c) transferência de arquivo *both-ways* (em ambos os sentidos)

d) acesso interativo;

e) acesso à rede dependente de horário do dia ou de data.

9.4.8 Controle de roteamento da rede

Redes compartilhadas, especialmente aquelas que cruzam as fronteiras da organização, podem exigir a incorporação de controles de roteamento para assegurar que as conexões entre computadores e os fluxos de informações não violem a política de controle de acesso das aplicações do negócio (ver 9.1). Este controle freqüentemente é essencial para redes compartilhadas com terceiros (usuários que não pertencem à organização).

Os controles de roteamento devem ser baseados em mecanismos de verificação positiva de endereços de origem e destino. A tradução dos endereços de rede também é um mecanismo muito útil para isolar redes e impedir as rotas de propagarem da rede de uma organização para a rede de outra. Eles podem ser implementados em software ou hardware. Os implementadores devem estar conscientes quanto à robustez de quaisquer mecanismos adotados.

9.4.9 Segurança de serviços em rede

Uma vasta gama de serviços de redes públicas ou privadas está disponível, alguns dos quais oferecem serviços com valor agregado. Os serviços de rede podem ter características de segurança únicas ou complexas. As organizações que usam serviços de rede devem se assegurar de que uma descrição clara dos atributos de segurança de todos os serviços usados seja fornecida.

9.5 Controle de acesso ao sistema operacional

Objetivo: Impedir acesso não autorizado a computadores.

As facilidades de segurança no nível de sistema operacional devem ser usadas para restringir o acesso aos recursos dos computadores. Estas facilidades devem ser capazes de:

a) identificar e confirmar a identidade, e se necessário o terminal ou localização, de cada usuário autorizado;

b) registrar acessos ao sistema bem-sucedidos e fracassados;

c) fornecer os meios apropriados para autenticação; se for usado um sistema de gerenciamento de senhas, ele deve garantir senhas de qualidade [ver 9.3.1 d)].

d) onde apropriado, restringir os tempos de conexão dos usuários.

Outros métodos de controle de acesso, tais como “challenge-response”, estão disponíveis se forem justificáveis com base no risco para o negócio.

9.5.1 Identificação automática de terminal

Identificação automática de terminais deve ser considerada para autenticar conexões com locais específicos e com equipamentos portáteis. Identificação automática de terminais é uma técnica que pode ser usada se for importante que a sessão possa ser iniciada apenas de um local específico ou de um terminal de computador específico. Um identificador no terminal, ou acoplado ao terminal, pode ser usado para indicar se este terminal em particular está autorizado a iniciar ou receber transações específicas.

Pode ser necessário aplicar proteção física ao terminal, para manter a segurança do identificador do terminal. Diversas outras técnicas também podem ser usadas para autenticar usuários (ver 9.4.3).

9.5.2 Procedimentos de logon em terminais

O acesso a serviços de informação deve ser realizado via um processo de *logon* seguro. O procedimento para conectar em um sistema de computador deve ser projetado para minimizar a oportunidade de acessos não autorizados. O procedimento de *logon* deve, portanto, divulgar o mínimo de informações sobre o sistema, de forma a evitar fornecer assistência desnecessária a um usuário não autorizado. Um bom procedimento de *logon* deve:

a) não exibir identificadores do sistema ou do aplicativo até que o processo de *logon* tenha sido completado com sucesso;

b) exibir um aviso genérico de que o computador deve ser acessado apenas por usuários autorizados;

c) não fornecer mensagens de *help* durante o procedimento de *logon* que poderiam ajudar um usuário não autorizado;

d) validar as informações de *logon* apenas após terminada toda a entrada de dados. Se ocorrer uma condição de erro, o sistema não deve indicar qual parte dos dados está correta ou incorreta;

e) limitar a quantidade permitida de tentativas fracassadas de *logon* (recomenda-se três) e considerar:

   1) registrar todas as tentativas fracassadas;
   2) forçar um intervalo de tempo antes que tentativas adicionais de *logon* sejam permitidas ou rejeitar quaisquer tentativas adicionais sem autorização específica;
   3) desconectar as conexões de *links* de dados;

f) limitar o tempo mínimo e máximo permitidos para o procedimento de *logon*. Se excedido, o sistema deve encerrar o *logon*;

g) exibir as seguintes informações na conclusão de um *logon* bem-sucedido:

   1) data e hora do *logon* anterior bem-sucedido;
   2) detalhes de quaisquer tentativas de *logon* fracassadas desde o último *logon* bem-sucedido.

9.5.3 Identificação e autenticação de usuários

Todos os usuários (incluindo equipe de suporte técnico, tais como operadores, administradores de rede, programadores de sistema e administradores de banco de dados) devem ter um identificador exclusivo (ID de usuário) para seu uso pessoal, de modo que as atividades possam ser rastreadas até o responsável individual. As IDs de usuário não devem dar nenhuma indicação do nível de privilégio do usuário (ver 9.2.2), por exemplo gerente ou supervisor.

Em circunstâncias excepcionais, onde existir um benefício claro para o negócio, o uso de uma ID de usuário compartilhada para um grupo de usuários ou um serviço

específico pode ser adequado. A aprovação da gerência deve ser documentada para estes casos. Controles adicionais podem ser exigidos para manter a responsabilização.

Existem vários processos de autenticação que podem ser usados para substanciar a identidade alegada de um usuário. Senhas (ver também 9.3.1 e abaixo) são um modo muito usual de fornecer identificação e autenticação (I&A) baseado em um segredo que apenas o usuário conhece. O mesmo também pode ser conseguido através de meios criptográficos e protocolos de autenticação.

Objetos tais como *tokens* de memória ou *smartcards* que os usuários portem consigo também podem ser usados para I & A. Tecnologias de autenticação biométrica, que usam as características únicas ou atributos de um indivíduo, também podem ser usadas para autenticar a identidade da pessoa. Uma combinação de tecnologias e mecanismos associados de forma segura resultará em autenticação mais poderosa.

9.5.4 Sistema de gerenciamento de senhas

As senhas são um dos principais meios de validar a autoridade de um usuário para acessar um serviço informatizado. Sistemas de gerenciamento de senhas devem prover uma funcionalidade eficaz e interativa que assegure senhas de qualidade (ver 9.3.1 para orientação sobre o uso de senhas).

Algumas aplicações exigem que senhas sejam atribuídas por uma autoridade independente. Na maioria dos casos as senhas são selecionadas e alteradas pelos usuários.

Um bom sistema de gerenciamento de senhas deve:

a) obrigar o uso de senhas individuais para manter a responsabilização;

b) onde apropriado, permitir aos usuários selecionar e alterar suas próprias senhas e incluir um procedimento de confirmação para permitir corrigir erros de digitação;

c) obrigar a escolha de senhas de qualidade, como descrito no item 9.3.1;

d) onde usuários alteram suas próprias senhas, obrigar alterações de senha como descrito no item 9.3.1;

e) onde os usuários selecionam as senhas, forçá-los a alterar senhas temporárias no primeiro *logon* (ver 9.2.3);

f) manter um registro de senhas anteriores dos usuários, por exemplo pelos 12 meses anteriores, e impedir a reutilização;

g) não exibir senhas na tela quando estiverem sendo digitadas;

h) armazenar arquivos de senhas separadamente dos dados das aplicações do sistema;

i) armazenar senhas sob forma criptografada usando um algoritmo de criptografia *one-way*;

j) alterar as senhas *default* dos fornecedores em seguida à instalação dos softwares.

9.5.5 Uso de utilitários do sistema

A maioria das instalações de computador tem um ou mais programas utilitários de sistema que podem ser capazes de sobrepujar controles dos sistemas e aplicativos. É essencial que o uso deles seja restrito e controlado à risca. Os seguintes controles devem ser considerados:

a) uso de procedimentos de autenticação para utilitários de sistema;
b) segregar os utilitários dos softwares aplicativos;
c) limitação do uso de utilitários de sistema à quantidade mínima praticável de usuários autorizados e confiáveis;
d) autorização para uso *ad hoc* de utilitários de sistema;
e) limitação da disponibilidade dos utilitários de sistema, por exemplo pela duração de uma modificação autorizada;
f) registro em *log* de todo uso de utilitários de sistema;
g) definir e documentar níveis de autorização para utilitários de sistema;
h) remover todos os softwares utilitários e softwares de sistema que sejam desnecessários.

9.5.6 Alarme de coação para salvaguardar usuários

A provisão de um alarme de coação deve ser considerada para usuários que possam ser alvo de coerção. A decisão de se colocar um tal alarme deve ser baseada em uma avaliação de riscos. Devem ser definidas responsabilidades e procedimentos para responder a um alarme de coação.

9.5.7 Time-out no terminal

Terminais inativos em locais de alto risco, por exemplo áreas públicas ou externas fora do gerenciamento de segurança da organização, ou servindo a sistemas de alto risco, devem ser desligados *(shut-down)* após um período definido de inatividade, para impedir o acesso de pessoas não autorizadas. Este recurso deve limpar a tela do terminal e fechar as sessões do aplicativo e da rede após um período definido de inatividade. O intervalo de tempo deve refletir os riscos de segurança da área e dos usuários do terminal.

Uma forma limitada de facilidade de *time-out* de terminal pode ser fornecida em alguns PCs que limpam a tela e impedem o acesso não autorizado mas não fecham as sessões da rede ou do aplicativo.

9.5.8 Limitação de tempo de conexão

Restrições nos tempos de conexão devem fornecer segurança adicional para aplicações de alto risco. Limitar o período durante o qual são permitidas conexões de terminal a serviços informatizados reduz a janela de oportunidade para acesso não autorizado. Um tal controle deve ser considerado para aplicações sensíveis de computador, especialmente aquelas com terminais instalados em locais de alto risco, tais como áreas públicas ou externas que estão fora do gerenciamento de segurança da organização. Exemplos de tais restrições incluem:

a) usar *slots* de tempo predeterminados, por exemplo para transmissões de arquivo em *batch* ou sessões interativas normais de curta duração;

b) restringir horários de conexão às horas normais de expediente se não houver necessidade de horas extras ou operação em horário estendido.

9.6 Controle de Acesso às Aplicações

Objetivo: Impedir acesso não autorizado às informações mantidas nos sistemas de informação. Os recursos de segurança devem ser usados para restringir o acesso dentro dos sistemas aplicativos. O acesso lógico ao software e às informações deve ser restrito aos usuários autorizados. Os sistemas aplicativos devem: a) controlar o acesso dos usuários às informações e funções do sistema aplicativo, de acordo com uma política de controle de acesso definida; b) fornecer proteção contra acesso não autorizado para qualquer software utilitário e de sistema operacional que seja capaz de fazer *override* nos controles do sistema ou aplicativo; c) não comprometer a segurança de outros sistemas com os quais sejam compartilhados recursos de informação; d) ter capacidade de fornecer acesso às informações apenas para o proprietário, outros indivíduos nomeados autorizados ou grupos de usuários definidos.

9.6.1 Restrição de acesso às informações

Usuários de sistemas aplicativos, incluindo a equipe de suporte, devem receber acesso às informações e funções dos sistemas aplicativos de acordo com uma política predefinida de controle de acesso, baseada nos requisitos individuais das aplicações do negócio e consistente com a política organizacional de acesso a informações (ver 9.1). A aplicação dos seguintes controles deve ser considerada de forma a suportar as exigências de restrição de acesso:

a) fornecer menus para controlar o acesso a funções dos sistemas aplicativos;

b) restringir o conhecimento dos usuários sobre informações ou funções dos sistemas aplicativos que eles não estão autorizados a acessar, com "censura" apropriada da documentação de usuário;

c) controlar os direitos de acesso dos usuários, como ler, gravar, apagar ou executar;

d) garantir que as saídas produzidas pelos sistemas aplicativos, que tratam informações sensíveis, contenham apenas as informações que são relevantes para o uso das saídas e sejam enviadas apenas para terminais e locais autorizados, incluindo revisão periódica de tais saídas para garantir que informações redundantes sejam removidas.

9.6.2 Isolamento de sistemas sensíveis

Sistemas sensíveis podem exigir um ambiente computacional dedicado (isolado). Alguns sistemas aplicativos são suficientemente sensíveis a perdas potenciais a ponto de exigir tratamento especial. A sensibilidade pode indicar que o sistema aplicativo deve ser executado em um computador dedicado, deve compartilhar recursos apenas com sistemas aplicativos confiáveis ou não ter limitações. As seguintes considerações se aplicam:

a) A sensibilidade de um sistema aplicativo deve ser explicitamente identificada e documentada pelo proprietário da aplicação (ver 4.1.3).

b) Quando uma aplicação sensível é executada em um ambiente compartilhado, os sistemas aplicativos com os quais ela compartilhará recursos devem ser identificados e acordados com o proprietário da aplicação sensível.

9.7 Monitorando o acesso e o uso do sistema

Objetivo: Detectar atividades não autorizadas. Os sistemas devem ser monitorados para detectar desvios da política de controle de acesso e registrar eventos monitoráveis para fornecer provas no caso de incidentes de segurança. O monitoramento do sistema permite que a eficácia dos controles adotados seja verificada e que a conformidade com o modelo de política de acesso (ver 9.1) seja confirmada.

9.7.1 Registro de eventos em log

Logs para auditoria, que registrem exceções e outros eventos relevantes para a segurança, devem ser produzidos e mantidos por um período acordado para auxiliar investigações futuras e monitorar controle de acessos. Os *logs* para auditoria devem incluir também:

a) IDs de usuários

b) datas e horários de *logon* e *logoff*;

c) identidade ou localização do terminal, se possível;

d) registros das tentativas de acesso ao sistema, bem-sucedidas e rejeitadas;

e) registros das tentativas de acesso a dados e outros recursos, bem-sucedidas e rejeitadas.

Pode ser exigido que determinados *logs* de auditoria sejam arquivados como parte da política de retenção de registros ou devido à necessidade de coletar provas (ver também cláusula 12).

9.7.2 Monitorando o uso do sistema

9.7.2.1 *Procedimentos e áreas de risco*

Devem ser implantados procedimentos para monitorar o uso de facilidades de processamento de informações. Tais procedimentos são necessários para garantir que os usuários estejam executando apenas atividades que foram explicitamente autorizadas. O nível de monitoramento exigido para as facilidades individuais deve ser determinado por uma avaliação de riscos. As áreas que devem ser consideradas incluem:

a) acesso autorizado, incluindo detalhes tais como:

   1) a ID do usuário;
   2) a data e o horário de eventos importantes;
   3) os tipos de eventos;
   4) os arquivos acessados;
   5) o programa/utilitários usados;

b) todas operações privilegiadas, tais como:

   1) uso de uma conta de supervisor;
   2) início *(start-up)* e fim *(stop)* do sistema;
   3) *attach*/*detach* de dispositivo de I/O;

c) tentativas de acesso não autorizadas, tais como:

   1) tentativas fracassadas;
   2) violações da política de acesso e notificações para *gateways* e *firewalls* da rede;
   3) alertas originados por sistemas proprietários de detecção de intrusão;

d) alertas ou falhas de sistema tais como:

   1) mensagens ou alertas de console;
   2) exceções de *log* do sistema
   3) alarmes de gerenciamento da rede.

9.7.2.2 *Fatores de risco*

O resultado do monitoramento das atividades deve ser examinado regularmente. A freqüência do exame depende dos riscos envolvidos. Os fatores de risco que devem ser considerados incluem:

a) a criticalidade dos processos das aplicações;

b) o valor, confidencialidade ou criticalidade das informações envolvidas;

c) a experiência passada de infiltração e má utilização do sistema;

d) a extensão das interconexões do sistema (particularmente redes públicas).

9.7.2.3 *Registrando e revisando eventos*

Uma revisão do *log* de eventos envolve o entendimento das ameaças enfrentadas pelo sistema e da maneira como elas surgem. Exemplos de eventos que podem exigir investigação adicional no caso de incidentes de segurança são apresentados no item 9.7.1.

Os *logs* de sistema geralmente contêm um grande volume de informações, muitas das quais são irrelevantes para o monitoramento do sistema. Para ajudar a identificar os eventos significativos para os fins de monitoramento de segurança, deve ser

considerada a cópia automática dos tipos de mensagens apropriados para um segundo *log*, e/ou o uso de utilitários de sistema adequados ou ferramentas de auditoria para executar o exame do arquivo.

Quando for feita a alocação de responsabilidade para revisão do *log*, deve ser considerada uma separação de papéis entre as pessoas que executam a revisão e aquelas cujas atividades estão sendo monitoradas.

Atenção particular deve ser dada à segurança do recurso de *log*, porque se adulterado ele pode dar uma falsa sensação de segurança. Os controles devem ter como objetivo proteger contra alterações não autorizadas e problemas operacionais, incluindo:

a) o recurso de *log* ser desativado;

b) alterações nos tipos de mensagens que são gravadas;

c) arquivos *logs* serem alterados ou apagados;

d) a mídia do arquivo *log* esgotar o espaço e deixar de gravar os eventos ou sobrescrever registros já gravados.

9.7.3 Sincronização de relógios

O acerto correto dos relógios dos computadores é importante para assegurar a exatidão dos *logs* para auditoria, que podem ser exigidos para investigações ou como prova em casos legais ou disciplinares. *Logs* de auditoria inexatos podem atrapalhar tais investigações e prejudicar a credibilidade de tais provas.

Onde um computador ou dispositivo de comunicação tiver a capacidade de operar um relógio tempo-real, ele deve ser colocado em um padrão acordado, por exemplo Tempo Universal Coordenado (UCT) ou tempo padrão local. Uma vez que alguns relógios podem desviar com o tempo, deve existir um procedimento para verificar e corrigir qualquer variação significativa.

9.8 Computação móvel e trabalho à distância

Objetivo: Assegurar segurança de informações no uso de computadores portáteis e facilidades de trabalho à distância. A proteção exigida deve ser compatível com os riscos que estes modos de trabalho específicos podem causar. Quando se usa computador portátil, os riscos de trabalhar em um ambiente não protegido devem ser considerados e a proteção apropriada deve ser aplicada. No caso de trabalho à distância, a organização deve aplicar proteção ao local onde é realizado o trabalho à distância e assegurar que condições adequadas estejam vigorando para este modo de trabalho.

9.8.1 Computadores portáteis

Quando se usa facilidades de computação móvel, tais como *notebooks*, *palmtops*, *laptops* e telefones móveis, cuidado especial deve ser tomado para garantir que as informações da organização não sejam comprometidas. Uma política formal deve ser adotada, levando em consideração os riscos de se trabalhar com facilidades de computação móvel, em particular em ambientes não protegidos. Por exemplo, tal política deve incluir os requisitos de proteção física, controles de acesso, técnicas

criptográficas, *backups* e proteção contra vírus. Esta política também deve incluir regras e conselhos sobre a conexão de dispositivos móveis a redes e orientação sobre o uso desses dispositivos em locais públicos.

Deve-se tomar cuidado quando se usa dispositivos portáteis de computação em locais públicos, salas de reunião e outras áreas não protegidas fora das instalações físicas da organização. Proteção deve estar implementada para evitar acesso não autorizado ou divulgação das informações armazenadas e processadas por estes dispositivos, por exemplo usando técnicas de criptografia (ver 10.3).

É importante que, quando tais dispositivos forem usados em locais públicos, seja tomado cuidado para evitar o risco de “bisbilhotagem” por pessoas não autorizadas. Procedimentos contra software malicioso devem ser implementados e devem ser mantidos sempre atualizados (ver 8.3). Deve estar disponível equipamento para possibilitar o *backup* rápido e fácil das informações. Estes *backups* devem receber proteção adequada contra roubo ou perda de informação, por exemplo.

Proteção adequada deve ser fornecida para uso de dispositivos portáteis conectados a redes. O acesso remoto às informações da organização através de rede pública usando dispositivos portáteis somente deve ocorrer após identificação e autenticação bem-sucedidas, e com mecanismos adequados de controle de acesso em vigor (ver 9.4).

Dispositivos de computação móvel também devem ser fisicamente protegidos contra roubo, especialmente quando deixados, por exemplo em carros e outros meios de transporte, quartos de hotel, centros de conferência e locais de reunião. Equipamentos que carregam informações importantes, confidenciais e/ou críticas para o negócio não devem ser deixados desacompanhados e, onde possível, devem ser fisicamente trancados em outro lugar, ou trancas especiais devem ser usadas para proteger o equipamento. Mais informações sobre proteção física de equipamentos móveis podem ser encontradas no item 7.2.5.

Deve ser feito um treinamento com a equipe que utiliza dispositivos portáteis para despertar sua conscientização sobre os riscos adicionais resultantes desta forma de trabalho e sobre os controles que devem ser implementados.

9.8.2 Trabalho à distância

O trabalho à distância usa tecnologia de telecomunicações para permitir aos funcionários trabalhar remotamente a partir de um local fixo, fora de sua organização. Proteção adequada do local do trabalho à distância deve ser implementada contra, por exemplo, o roubo do equipamento e de informações, a divulgação não autorizada de informações, o acesso remoto não autorizado aos sistemas internos da organização ou à utilização indevida dos equipamentos. É importante que o trabalho à distância seja autorizado e controlado pela gerência, e que arranjos adequados estejam vigorando para este modo de trabalho.

As organizações devem considerar o desenvolvimento de uma política, procedimentos e padrões para controlar as atividades de trabalho à distância. As organizações somente devem autorizar o trabalho à distância se elas estiverem satisfeitas que os arranjos de segurança e controles apropriados estão implantados e que estes obedecem à política de segurança da organização. O seguinte deve ser considerado:

a) a segurança física existente do local de trabalho à distância, levando em conta a segurança física do edifício e do ambiente local;

b) o ambiente proposto para o trabalho à distância;

c) os requisitos de segurança de comunicações, levando em conta a necessidade de acesso remoto aos sistemas internos da organização, a confidencialidade das informações que serão acessadas e transmitidas pelo *link* de comunicação e a confidencialidade do sistema interno;

d) a ameaça de acesso não autorizado a informações ou recursos por outras pessoas usando as acomodações, tais como familiares e amigos.

Os controles e arranjos a serem considerados incluem:

a) a provisão de equipamento e mobiliário adequados para as atividades de trabalho à distância;

b) uma definição do trabalho permitido, das horas de trabalho, da classificação das informações que podem ser retidas e dos sistemas e serviços internos que o funcionário que trabalha à distância está autorizado a acessar;

c) a provisão de equipamento de comunicação adequado, incluindo métodos para tornar seguro o acesso remoto;

d) segurança física;

e) regras e orientação sobre o acesso de familiares e visitantes ao equipamento e às informações;

f) a provisão de suporte e manutenção para o hardware e o software;

g) os procedimentos para *backup* e continuidade do negócio;

h) auditoria e monitoramento de segurança;

i) revogação de autoridade, direitos de acesso e a devolução do equipamento quando cessarem as atividades de trabalho à distância.

10 Desenvolvimento e manutenção de sistemas

10.1 Requisitos de segurança nos sistemas

Objetivo: Assegurar que a segurança seja embutida nos sistemas de informações.

Isto incluirá infra-estrutura, aplicações do negócio e aplicações desenvolvidas pelos usuários. O projeto e a implementação do processo corporativo que dá suporte à aplicação ou ao serviço pode ser crucial para a segurança. Os requisitos de segurança devem ser identificados e acordados antes do desenvolvimento de sistemas de informação.

Todos os requisitos de segurança, incluindo a necessidade de arranjos para *fallback*, devem ser identificados na fase de requisitos de um projeto e justificados, acordados e documentados como parte do “business case” geral para um sistema de informações.

10.1.1 Análise e especificação dos requisitos de segurança

Os relatórios com os requisitos do negócio para novos sistemas, ou melhorias em sistemas existentes, devem especificar as necessidades de controles. Tais

especificações devem considerar os controles automatizados a serem incorporados no sistema e a necessidade de suportar controles manuais. Considerações similares devem ser aplicadas ao se avaliar pacotes de software para aplicações do negócio. Se considerado apropriado, a gerência pode desejar utilizar produtos certificados e avaliados de forma independente.

Os requisitos de segurança e controles devem refletir o valor para o negócio dos ativos de informação envolvidos e o prejuízo potencial para o negócio, que poderia resultar de uma falha ou ausência de segurança. A base para se analisar os requisitos de segurança e identificar os controles para satisfazê-los é a avaliação de riscos e gerenciamento de riscos.

Os controles introduzidos no estágio de projeto são significativamente mais baratos de se implementar e manter do que aqueles incluídos durante ou após a implementação.

10.2 Segurança em sistemas aplicativos

Objetivo: Impedir perda, modificação ou má utilização de dados dos usuários em sistemas aplicativos. Controles apropriados e *audit trails* ou *logs* de atividade devem ser projetados nos sistemas aplicativos, incluindo aplicativos escritos pelos usuários. Estes devem incluir a validação de dados de entrada, dados de processamento interno e dados de saída.

Controles adicionais podem ser exigidos para sistemas que processam, ou têm impacto em, ativos confidenciais, valiosos ou críticos da organização. Tais controles devem ser determinados com base nos requisitos do sistema e na avaliação de riscos.

10.2.1 Validação dos dados de entrada

A entrada de dados para os sistemas aplicativos deve ser validada para garantir que está correta e apropriada. Verificações devem ser aplicadas à entrada de transações comerciais, dados cadastrais (nomes e endereços, limites de crédito, números de referência de clientes) e tabelas de parâmetros (listas de preços, taxas de conversão de moeda, taxas de impostos). Os seguintes controles devem ser considerados:

a) entrada dupla ou outras verificações de entrada para detectar os seguintes erros:
   1) valores fora da faixa;
   2) caracteres inválidos nos campos de dados;
   3) dados não informados ou incompletos;
   4) limites inferior e superior de volumes de dados excedidos;
   5) dados de controle não autorizados ou inconsistentes;

b) revisão periódica do conteúdo dos campos-chaves ou arquivos de dados mais importantes, para confirmar sua validade e integridade;

c) inspecionar documentos de entrada impressos quanto a quaisquer alterações não autorizadas nos dados de entrada (todas as alterações em documentos de entrada devem ser autorizadas);

d) procedimentos para responder a erros de validação;

e) procedimentos para testar a plausibilidade dos dados de entrada;

f) definir as responsabilidades de todo o pessoal envolvido no processo de entrada de dados.

10.2.2 Controle do processamento interno

10.2.2.1 *Áreas de risco*

Dados que foram entrados corretamente podem ser corrompidos por erros de processamento ou através de atos deliberados. Verificações para validação devem ser incorporadas nos sistemas para detectar tal corrompimento. O projeto das aplicações deve assegurar que sejam implementadas restrições para minimizar o risco de falhas de processamento que levem a uma perda de integridade. As áreas específicas a serem consideradas incluem:

a) o uso e a localização nos programas de funções de inclusão e exclusão para implementar alterações nos dados;

b) os procedimentos para impedir que os programas executem na ordem errada ou executem após falha de um processamento anterior (ver também 8.1.1);

c) o uso de programas corretos para recuperar de falhas e garantir o processamento correto dos dados.

10.2.2.2 *Verificações e controles*

Os controles exigidos dependerão da natureza do aplicativo e do impacto nos negócios causados por quaisquer dados corrompidos. Exemplos de verificações que podem ser incorporadas incluem os seguintes:

a) controles de sessão ou de lotes, para conciliar arquivos de dados após atualizações de transações;

b) fechamento dos controles, para verificar saldos inicias contra saldos finais anteriores, a saber:
   1) controles de execução-para-execução
   2) totais da atualização dos arquivos;
   3) controles de programa-para-programa;

c) validação de dados gerados pelo sistema (ver 10.2.1);

d) verificações da integridade de dados ou softwares transmitidos ou recebidos, entre computadores central e remotos (ver 10.3.3);

e) totais *hash* de registros e arquivos;

f) verificações para assegurar que os programas aplicativos sejam executados na hora correta;

g) verificações para assegurar que os programas sejam executados na ordem correta e encerrados no caso de uma falha, e que processamento posterior seja suspenso até o problema ser resolvido.

10.2.3 Autenticação de mensagens

Autenticação de mensagens é uma técnica usada para detectar alterações não autorizadas ou corrompimento dos conteúdos de uma mensagem transmitida

eletronicamente. Ela pode ser implementada em hardware ou software que suporte um dispositivo físico de autenticação de mensagens ou um algoritmo de software.

Autenticação de mensagens deve ser considerada para aplicativos onde exista uma necessidade de segurança para proteger a integridade do conteúdo das mensagens; por exemplo, transferência eletrônica de fundos, especificações, contratos e propostas com alta importância ou outros intercâmbios de dados eletrônicos similares. Uma avaliação dos riscos de segurança deve ser efetuada para determinar se é exigida autenticação de mensagens e para identificar o método mais apropriado de implementação.

Autenticação de mensagens não se destina a proteger os conteúdos de uma mensagem contra divulgação não autorizada. Técnicas de criptografia (ver 10.3.2 e 10.3.3) podem ser usadas como um meio adequado de implementar autenticação de mensagens.

10.2.4 Validação dos dados de saída

A saída de dados de um sistema aplicativo deve ser validada para garantir que o processamento de informações armazenadas seja correto e apropriado às circunstâncias. Geralmente, os sistemas são construídos baseado na premissa de que tendo havido validação apropriada, confirmação e testes, a saída será sempre correta. Isto não é sempre verdadeiro. A validação das saídas pode incluir:

a) verificações de plausibilidade para testar se os dados da saída são razoáveis;

b) contadores de controle para conciliação, para assegurar o processamento de todos os dados;

c) fornecer informações suficiente para que um leitor ou um sistema de processamento subsequente possa determinar a exatidão, a inteireza, a precisão e a classificação das informações;

d) procedimentos para responder aos testes de validação de saída;

e) definir as responsabilidades de todo o pessoal envolvido no processo de saída de dados.

10.3 Controles criptográficos

Objetivo: Proteger a confidencialidade, autenticidade ou integridade das informações. Sistemas e técnicas criptográficas devem ser usados para a proteção das informações que sejam consideradas em risco e para as quais outros controles não propiciam proteção adequada.

10.3.1 Política para o uso de controles criptográficos

A tomada de decisão sobre se uma solução criptográfica é apropriada deve ser vista como uma parte de um processo mais amplo de avaliação de riscos e seleção de controles. Uma avaliação de riscos deve ser efetuada para determinar o nível de proteção que as informações devem receber. Esta avaliação pode então ser usada para determinar se um controle criptográfico é apropriado, que tipo de controle deve ser aplicado e para quais propósitos e processos do negócio.

Uma organização deve desenvolver uma política sobre o uso de controles criptográficos para proteção de suas informações. Uma tal política é necessária para maximizar os benefícios e minimizar os riscos de usar técnicas criptográficas, e evitar uso inapropriado ou incorreto. No desenvolvimento desta política, o seguinte deve ser considerado:

a) a abordagem gerencial quanto ao uso de controles criptográficos em toda a organização, incluindo os princípios gerais sob os quais as informações do negócio devem ser protegidas;

b) a abordagem para o gerenciamento de chaves, incluindo métodos para lidar com a recuperação de informações criptografadas no caso de chaves perdidas, comprometidas ou danificadas;

c) papéis e responsabilidades, por exemplo quem é responsável por:

d) a implementação da política;

e) o gerenciamento das chaves;

f) como deve ser determinado o nível de proteção criptográfica apropriado;

g) os padrões a serem adotados para a implementação efetiva em toda a organização (qual solução será usada para quais processos do negócio).

10.3.2 Criptografia

Criptografia é uma técnica que pode ser usada para proteger a confidencialidade das informações. Ele deve ser considerada para proteção de informações sensíveis ou críticas.

O nível requerido de proteção deve ser identificado com base em uma avaliação de riscos, levando-se em conta o tipo e a qualidade do algoritmo de criptografia usado e a tamanho das chaves criptográficas a serem usadas.

Ao se implementar a política de criptografia da organização, devem ser considerados os regulamentos e as restrições nacionais que podem se aplicar ao uso de técnicas criptográficas em diferentes partes do mundo e às questões de fluxo de informações criptografadas entre países. Além disso, deve ser dada consideração aos controles que se aplicam à exportação e importação de tecnologia criptográfica (ver também 12.1.6).

Deve ser buscada consultoria especializada para identificar o nível de proteção apropriado, para selecionar produtos adequados que fornecerão a proteção requerida e a implementação de um sistema seguro de gerenciamento de chaves (ver também 10.3.5). Além disso, pode ser necessário buscar consultoria jurídica relacionada às leis e regulamentos que possam se aplicar ao uso que a organização pretende fazer da criptografia.

10.3.3 Assinaturas digitais

As assinaturas digitais fornecem um meio de proteger a autenticidade e a integridade de documentos eletrônicos. Por exemplo, elas podem ser usados no comércio eletrônico, onde houver necessidade de confirmar quem assinou um documento eletrônico e de verificar se os conteúdos do documento assinado foram alterados.

Assinaturas digitais podem ser aplicadas a qualquer forma de documento processado eletronicamente; por exemplo, elas podem ser usadas para assinar pagamentos eletrônicos, transferências de fundos, contratos e acordos. Assinaturas digitais podem ser implementadas usando uma técnica criptográfica baseada em um par de chaves relacionadas de forma única, onde uma chave é usada para criar a assinatura (a chave privada) e a outra para verificar a assinatura (a chave pública).

Deve ser tomado cuidado para proteger a confidencialidade da chave privada. Esta chave deve ser mantida em segredo, já que qualquer um que tenha acesso a esta chave pode assinar documentos, como pagamentos e contratos, falsificando desta forma a assinatura do proprietário daquela chave. Além disso, proteger a integridade da chave pública é importante. Esta proteção é fornecida pelo uso de um certificado de chave pública (ver 10.3.5).

É preciso levar em consideração o tipo e a qualidade do algoritmo de assinatura usado e o tamanho das chaves a serem usadas. As chaves criptográficas usadas para assinaturas digitais devem ser diferentes daquelas usadas para criptografia de dados (ver 10.3.2).

Quando se usar assinaturas digitais, deve ser levada em consideração qualquer legislação pertinente que descreva as condições sob as quais uma assinatura digital é legalmente válida. Por exemplo, no caso de comércio eletrônico é importante conhecer a situação legal de assinaturas digitais. Pode ser necessário ter contratos legalmente válidos ou outros acordos para suportar o uso de assinaturas digitais onde o embasamento legal for inadequado. Deve ser buscada consultoria jurídica sobre as leis e regulamentos que possam se aplicar ao uso que a organização pretende fazer das assinaturas digitais.

10.3.4 Serviços de não-repudiação

Serviços de não-repudiação devem ser usados, onde possa ser necessário, para resolver disputas sobre a ocorrência ou não ocorrência de um evento ou ação, por exemplo uma disputa envolvendo o uso de uma assinatura digital em um contrato ou pagamento eletrônico. Eles podem ajudar a estabelecer provas para substanciar se um determinado evento ou ação ocorreu, por exemplo negação de envio de uma instrução assinada eletronicamente usando correio eletrônico. Estes serviços são baseados no uso de técnicas de criptografia e assinatura digital (ver também 10.3.2 e 10.3.3).

10.3.5 Gerenciamento de chaves

10.3.5.1 *Proteção de chaves criptográficas*

O gerenciamento das chaves criptográficas é essencial para o uso eficaz das técnicas de criptografia. Qualquer comprometimento ou perda das chaves criptográficas pode levar a um comprometimento da confidencialidade, autenticidade e/ou integridade das informações. Um sistema de gerenciamento deve ser implantado para dar suporte à organização no uso dos dois tipos de técnicas criptográficas, que são:

a) técnicas de chave secreta, onde duas ou mais partes compartilham a mesma chave e esta chave é usada tanto para criptografar quanto para descriptografar as informações. Esta chave tem que ser mantida secreta uma vez que qualquer

um que tenha acesso a ela é capaz de descriptografar todas as informações que foram codificadas com esta chave, ou introduzir informações não autorizadas;

b) técnicas de chave pública, onde cada usuário tem um par de chaves, uma chave pública (que pode ser revelada a qualquer um) e uma chave privada (que tem que ser mantida em segredo). As técnicas de chave pública podem ser usadas para criptografia (ver 10.3.2) e para produzir assinaturas digitais (ver 10.3.3).

Todas as chaves devem ser protegidas contra modificação e destruição, e chaves secretas e privadas precisam de proteção contra divulgação não autorizada. Técnicas criptográficas também podem ser usadas para este propósito. Proteção física deve ser usada para proteger o equipamento usado para gerar, armazenar e arquivar as chaves.

10.3.5.2 *Padrões, procedimentos e métodos*

Um sistema de gerenciamento de chaves deve ser baseado em um conjunto acordado de padrões, procedimentos e métodos seguros para:

a) gerar chaves para sistemas criptográficos diferentes e aplicações diferentes;

b) gerar e obter certificados de chaves públicas;

c) distribuir chaves para os usuários pretendidos, incluindo como as chaves devem ser ativadas ao serem recebidas;

d) armazenar chaves, incluindo como os usuários autorizados obterão acesso às chaves;

e) alterar ou atualizar chaves, incluindo regras sobre quando as chaves devem ser mudadas e como isto será feito;

f) revogar chaves, incluindo como as chaves devem ser retomadas ou desativadas, por exemplo quando as chaves forem comprometidas ou quando um usuário deixar a organização (em cujo caso as chaves também deve ser colocadas em *archive*);

g) recuperar chaves que estão perdidas ou corrompidas como parte do gerenciamento da continuidade do negócio; por exemplo. para recuperação de informações criptografadas;

h) guardar chaves em *archives*, por exemplo, para informações que estão gravadas em *archives* ou em *backups*.

i) destruir chaves;

j) *log* e auditoria de atividades relacionadas com gerenciamento de chaves.

Para reduzir a probabilidade de comprometimento, as chaves devem ter datas definidas de ativação e desativação de modo que possam ser usadas apenas por um período limitado de tempo. Este período de tempo deve ser dependente das circunstâncias em que o controle criptográfico está sendo usado e do risco percebido.

Pode ser necessário considerar procedimentos para tratar solicitações legais de acesso às chaves criptográficas; por exemplo, pode ser necessário disponibilizar informações criptografadas em formato descriptografado como prova em uma questão na justiça.

Além da questão de chaves secretas e privadas gerenciadas de forma segura, a proteção das chaves públicas também deve ser considerada. Existe uma ameaça de alguém forjar uma assinatura digital substituindo uma chave pública do usuário por

uma chave sua. Este problema é tratado pelo uso de um certificado de chave pública. Estes certificados devem ser produzidos de uma maneira que associe informações relativas ao proprietário do par de chaves pública/privada com a chave pública. Portanto, é importante que se possa confiar no processo de gerenciamento que gera estes certificados. Este processo é normalmente conduzido por uma autoridade de certificação, que deve ser uma organização reconhecida com controles adequados e procedimentos implantados para propiciar o grau exigido de confiança.

Os conteúdos de acordos ou contratos de níveis de serviço com fornecedores externos de serviços criptográficos, como uma autoridade de certificação, devem cobrir as questões de responsabilidades, confiabilidade dos serviços e tempos de resposta para o provimento dos serviços (ver 4.2.2).

10.4 Segurança de arquivos do sistema

Objetivo: Assegurar que os projetos de IT e atividades de suporte sejam conduzidos de uma forma segura. O acesso aos arquivos do sistema deve ser controlado.

Manter a integridade do sistema deve ser responsabilidade da função usuária ou grupo de desenvolvimento ao qual o sistema aplicativo ou software pertence.

10.4.1 Controle de software operacional

Deve ser fornecido controle para a implementação de software em sistemas operacionais. Para minimizar os riscos de corrupção de sistemas operacionais, os seguintes controles devem ser considerados:

a) A atualização de bibliotecas de programas operacionais deve ser executada somente por um bibliotecário indicado sob autorização da gerência apropriada (ver 10.4.3).

b) Se possível, os sistemas operacionais devem ter apenas código executável.

c) O código executável não deve ser implementado em um sistema operacional até prova de que os testes foram bem-sucedidos e de que a aceitação do usuário foi obtida, e de que as correspondentes bibliotecas-fontes de programas foram atualizadas;

d) Deve ser mantido um *log* para auditoria de todas as atualizações feitas nas bibliotecas de programas operacionais.

e) Versões anteriores do software devem ser guardadas como medida de contingência.

Software usado em sistemas operacionais, que seja fornecido pelo revendedor, deve ser mantido em um nível no qual o fornecedor dá suporte. Qualquer decisão de fazer *upgrade* para uma nova versão deve levar em conta a segurança da versão, isto é, a introdução de nova funcionalidade de segurança ou a quantidade e a severidade dos problemas de segurança que afetam esta versão. *Software patches* devem ser aplicados onde puderem ajudar a remover ou reduzir fraquezas na segurança.

Acesso lógico ou físico deve ser dado aos fornecedores apenas para fins de suporte quando necessário, e com a aprovação da gerência. As atividades do fornecedor devem ser monitoradas.

10.4.2 Proteção de dados usados em teste de sistemas

Dados de teste devem ser protegidos e controlados. Os testes e a aceitação de sistemas geralmente exigem volumes substanciais de dados de teste que sejam o mais parecido possível com os dados operacionais. O uso de bancos de dados operacionais contendo informações pessoais deve ser evitado. Se tais informações forem usadas, elas devem ser despersonalizadas antes do uso. Os seguintes controles devem ser aplicados para proteger dados operacionais, quando usados para fins de teste:

a) Os procedimentos de controle de acesso, que se aplicarem aos sistemas aplicativos de produção, também devem ser aplicados aos sistemas aplicativos de teste.

b) Deve haver autorização separada a cada vez que informações de produção forem copiadas para um sistema aplicativo de teste.

c) Informações de produção devem ser apagadas do sistema aplicativo de teste imediatamente após o teste estar concluído.

d) A cópia e o uso de informações de produção deve ser registrada em *log* para fornecer uma *audit trail*.

10.4.3 Controle de acesso à biblioteca-fonte de programas

Para reduzir o potencial de corrompimento de programas de computador, deve ser mantido um controle estrito sobre o acesso às bibliotecas-fontes de programas, como se segue (ver também 8.3).

a) Onde possível, as bibliotecas-fontes de programas não devem ser mantidas nos sistemas operacionais;

b) Um bibliotecário para os programas deve ser nomeado para cada aplicação.

c) A equipe de suporte de IT não deve ter acesso irrestrito às bibliotecas-fontes de programas.

d) Programas em manutenção ou em desenvolvimento não devem ser mantidos em bibliotecas-fontes de programas de produção.

e) A atualização de bibliotecas-fontes de programas e a emissão de fontes de programas para os programadores devem ser executadas apenas pelo bibliotecário nomeado, com autorização do gerente de suporte de IT para a aplicação.

f) Listagens de programas devem ser guardadas em um ambiente seguro (ver 8.6.4).

g) Deve ser mantido um *log* para auditoria de todos os acessos às bibliotecas-fontes de programas.

h) Versões antigas de programas-fontes devem ser gravadas em *archives*, com uma indicação clara das datas e horários exatos de quando eles estavam operacionais, juntamente com todo o software de apoio, *job control*, definições de dados e procedimentos.

i) A manutenção e cópia de bibliotecas-fontes de programas devem estar sujeitas a procedimentos estritos de controle de alterações (ver 10.4.1).

10.5 Segurança nos processos de desenvolvimento e suporte

Objetivo: Manter a segurança dos softwares e das informações de sistemas aplicativos. Os ambientes de projeto e suporte devem ser estritamente controlados. Os gerentes responsáveis pelos sistemas aplicativos também devem ser responsáveis pela segurança do ambiente de projeto ou suporte. Eles devem assegurar que todas as alterações propostas nos sistemas sejam revisadas para verificar se elas não comprometem a segurança do sistema ou do ambiente operacional.

10.5.1 Procedimentos para controle de alterações

Para minimizar o corrompimento dos sistemas de informação, deve existir um controle estrito sobre a implementação de alterações. Procedimentos formais para controle de alterações devem ser obrigatórios. Eles devem garantir que os procedimentos de controle e segurança não sejam comprometidos, que os programadores do suporte recebam acesso apenas àquelas partes do sistema necessárias para seu trabalho, e que sejam obtidos um acordo e uma aprovação formais para cada alteração. Alterar software aplicativo pode impactar o ambiente operacional. Sempre que praticável, os procedimentos de controle de alterações operacionais e de aplicativos devem ser integrados (ver também 8.1.2). Este processo deve incluir:

a) manter um registro dos níveis de autorização acordados;

b) assegurar que as alterações sejam submetidas por usuários autorizados;

c) revisar procedimentos de controle e de integridade para garantir que eles não serão comprometidos pela alterações;

d) identificar todos os softwares de computador, as informações, as entidades de bancos de dados e hardware que precisam de modificação;

e) obter aprovação formal dos propósitos detalhados antes que o trabalho comece;

f) assegurar que o usuário autorizado aceite as alterações antes de qualquer implementação;

g) garantir que a implementação seja executada de forma a minimizar perturbações no negócio;

h) garantir que o conjunto de documentações do sistema seja atualizado na conclusão de cada alteração e que a documentação antiga seja arquivada ou descartada;

i) manter um controle de versão para todos os *updates* de software;

j) manter uma *audit trail* de todas as solicitações de alteração;

k) assegurar que a documentação operacional (ver 8.1.1) e os procedimentos dos usuários sejam alterados conforme necessário para ficarem adequadas;

l) assegurar que a implementação de alterações ocorra no momento certo e não perturbe os processos do negócio envolvidos.

Muitas organizações mantêm um ambiente onde os usuários testam novos softwares e que fica segregado dos ambientes de produção e desenvolvimento. Isto propicia um meio de ter controle sobre novos softwares e permite proteção adicional das informações operacionais que sejam usadas para fins de testes.

10.5.2 Revisão técnica de alterações em sistemas operacionais

Periodicamente, é necessário alterar o sistema operacional, por exemplo para instalar uma versão mais recente do software ou *patches* de alterações. Quando as alterações acontecem, os sistemas aplicativos devem ser revisados e testados para assegurar que não existe impacto adverso na operação ou na segurança. Este processo deve cobrir:

a) revisão dos procedimentos de controle de aplicativos e integridade, para garantir que eles não foram comprometidos pelas alterações no sistema operacional;

b) garantir que o plano de suporte anual e o orçamento cobrirão revisões e testes dos sistemas, resultantes de alterações no sistema operacional;

c) garantir que a notificação das alterações do sistema operacional seja fornecida em tempo para permitir que ocorram revisões apropriadas antes da implementação;

d) garantir que as alterações apropriadas sejam feitas nos planos de continuidade do negócio (ver cláusula 11).

10.5.3 Restrições para alterações em pacotes de software

Modificações em pacotes de software devem ser desencorajadas. Tanto quanto possível, e praticável, pacotes de software fornecidos por revendedor devem ser usados sem modificação. Onde for considerado essencial modificar um pacote de software, os seguintes pontos devem ser considerados:

a) o risco de controles embutidos e processos de integridade serem comprometidos;

b) se o consentimento do revendedor deve ser obtido;

c) a possibilidade de obter as alterações desejadas do próprio revendedor como atualizações padronizadas do software;

d) o impacto se a organização se tornar responsável pela manutenção futura do software como resultado das alterações.

Se alterações forem consideradas essenciais, o software original deve ser retido e as alterações aplicadas em uma cópia claramente identificadas. Todas as alterações devem ser completamente testadas e documentadas, de modo que possam ser reaplicadas se necessário em *upgrades* futuros do software.

10.5.4 “Covert channels” e código troiano

Um “covert channel” pode expor informações por alguns meios indiretos e obscuros. Ele pode ser ativado alterando-se um parâmetro acessível tanto por elementos seguros quanto inseguros de um sistema informatizado, ou embutindo-se informações em um fluxo de dados. Código troiano é projetado para afetar um sistema de uma forma que não é autorizada e não é prontamente percebida e não é solicitada pelo receptor ou usuário de um programa. “Covert channels” e código troiano raramente ocorrem por acidente. Onde existir preocupação com “covert channels” ou códigos troianos, os seguintes devem ser considerados:

a) comprar programas apenas de uma fonte de renome;
b) comprar programas em código-fonte apenas se o código puder ser verificado;
c) usar produtos testados e aprovados;
d) inspecionar todo o código-fonte antes do uso operacional;
e) controlar o acesso ao código e modificações no código após o código ser instalado;
f) usar equipe de confiança comprovada para trabalhar nos sistemas-chaves.

10.5.5 Desenvolvimento terceirizado de software

Onde o desenvolvimento de software for terceirizado, os seguintes pontos devem ser considerados:

a) contratos de licenciamento, propriedade do código e direitos de propriedade intelectual (ver 12.1.2);
b) certificação da qualidade e da exatidão do trabalho executado;
c) arranjos para serviços de custódia no caso de falta da terceira parte;
d) direitos de acesso para auditar a qualidade e exatidão do trabalho executado;
e) exigências contratuais para um código de qualidade;
f) testes antes da instalação para detectar código Troiano.

11 Gerenciamento da continuidade do negócio

11.1 Aspectos do gerenciamento da continuidade do negócio

Objetivo: Neutralizar interrupções nas atividades do negócio e proteger processos críticos do negócio contra os efeitos de grandes falhas ou desastres.

Um processo de gerenciamento da continuidade do negócio deve ser implementado para reduzir a perturbação causada por desastres e falhas de segurança (que podem ser resultantes de, por exemplo, desastres naturais, acidentes, falhas em equipamentos e ações deliberadas) a um nível aceitável através da combinação de controles preventivos e de recuperação.

As conseqüências de desastres, falhas de segurança e perda de serviços devem ser analisadas. Planos de contingência devem ser desenvolvidos e implementados para assegurar que os processos do negócio podem ser restaurados dentro das réguas de tempo exigidas. Tais planos devem ser atualizados e praticados para se tornarem uma parte integral de todos os outros processos de gerenciamento.

O gerenciamento da continuidade do negócio deve incluir controles para identificar e reduzir riscos, limitar as conseqüências de incidentes prejudiciais e garantir a retomada em tempo hábil das operações essenciais.

11.1.1 Processo de gerenciamento da continuidade do negócio

Deve existir um processo gerencial em vigor para desenvolver e manter a continuidade do negócio em toda a organização. Ele deve agregar os seguintes elementos chaves do gerenciamento da continuidade do negócio:

a) entender os riscos que a organização está enfrentando em termos de sua probabilidade e seu impacto, incluindo uma identificação e priorização dos processos críticos do negócio;

b) entender o impacto que provavelmente as interrupções terão sobre o negócio (é importante que sejam encontradas soluções que tratarão incidentes menores, bem como incidentes sérios que poderiam ameaçar a viabilidade da organização), e estabelecer os objetivos para o negócio das facilidades de processamento de informações;

c) considerar a contratação de seguro adequado, que pode formar parte do processo de continuidade do negócio;

d) formular e documentar uma estratégia de continuidade do negócio consistente com os objetivos e prioridades acordados para o negócio;

e) formular e documentar planos para continuidade do negócio em linha com a estratégia acordada;

f) testar e atualizar regularmente os planos e processos implementados;

g) assegurar que o gerenciamento da continuidade do negócio seja incorporado aos processos e à estrutura da organização. A responsabilidade pela coordenação do processo de gerenciamento da continuidade do negócio deve ser atribuída em um nível apropriado dentro da organização, por exemplo no fórum de segurança de informações (ver 4.1.1).

11.1.2 Continuidade do negócio e análise de impacto

A continuidade do negócio deve começar pela identificação de eventos que possam causar interrupções nos processos do negócio, tais como falhas em equipamento, incêndios e inundações. Isto deve ser seguido por uma avaliação de riscos para determinar o impacto daquelas interrupções (tanto em termos de escala de danos quanto de período para recuperação). Ambas estas atividades devem ser executadas com o total envolvimento dos proprietários dos recursos e processos do negócio. Esta avaliação considera todos os processos do negócio e não é limitada às facilidades de processamento de informações.

Dependendo dos resultados da avaliação de riscos, um plano estratégico deve ser desenvolvido para determinar o enfoque global para a continuidade do negócio. Uma vez que este plano tenha sido criado, ele deve ser endossado pela gerência.

11.1.3 Definição e implementação de planos de continuidade

Devem ser desenvolvidos planos para manter ou restaurar as operações do negócio nas réguas de tempo exigidas seguintes à interrupção, ou falha, nos processos críticos do negócio. O processo de planejamento da continuidade do negócio deve considerar o seguinte:

a) identificação e acordo sobre todas as responsabilidades e procedimentos emergenciais;
b) implementação de procedimentos emergenciais para permitir a recuperação e restauração dentro das réguas de tempo exigidas. É preciso dar atenção especial à avaliação de dependências externas do negócio e dos contratos em vigor;
c) documentação dos procedimentos e processos acordados;
d) educação apropriada da equipe nos procedimentos e processos para emergências, incluindo gerenciamento de crise;
e) testes e atualização dos planos.

O processo de planejamento deve focar nos objetivos requeridos do negócio, por exemplo restaurar serviços específicos para clientes em um período de tempo aceitável. Os serviços e recursos que permitirão que isto ocorra devem ser considerados, incluindo a mão-de-obra, recursos de processamento não relacionados a informações, bem como arranjos de *fallback* para as facilidades de processamento de informações.

11.1.4 Estrutura para o planejamento da continuidade do negócio

Deve ser mantida uma única estrutura para os planos de continuidade do negócio, para garantir que todos os planos sejam consistentes e para identificar prioridades para testes e manutenção. Cada plano de continuidade do negócio deve especificar claramente as condições para sua ativação, bem como os indivíduos responsáveis pela execução de cada componente do plano. Quando forem identificados novos requisitos, os procedimentos de emergência estabelecidos, tais como planos de evacuação ou quaisquer arranjos de *fallback* existentes, devem ser ajustados conforme apropriado.

Uma estrutura para planejamento de continuidade do negócio deve considerar o seguinte:

a) as condições para ativar os planos que descrevem o processo a ser seguido (como avaliar a situação, quem deve ser envolvido, etc.) antes de cada plano ser ativado;
b) procedimentos de emergência que descrevem as ações a serem tomadas em seguida a um incidente que coloca em risco as operações do negócio e/ou vidas humanas. Isto deve incluir arranjos para gerenciamento de relações públicas e

para ligação eficaz com as autoridades públicas apropriadas, tais como polícia, bombeiros e governo local;

c) procedimentos de *fallback* que descrevem as ações a serem tomadas para transferir as atividades essenciais do negócio ou serviços de apoio para locais alternativos temporários, e para colocar os processos do negócio de volta em operação dentro das réguas de tempo exigidas;

d) procedimentos de retomada que descrevem as ações a serem executadas para retornar às operações normais do negócio;

e) um cronograma de manutenção que especifica como e quando o plano será testado, e os processos para manter atualizado o plano;

f) atividades de conscientização e educação, que sejam projetadas para criar uma compreensão dos processos de continuidade do negócio e garantir que os processos continuem a ser eficazes;

g) as responsabilidades dos indivíduos, descrevendo quem é responsável por executar cada componente do plano. Alternativas devem ser indicadas conforme necessário.

Cada plano deve ter um proprietário específico. Procedimentos de emergência, planos de *fallback* manuais e planos de retomada devem estar dentro da responsabilidade dos proprietários dos recursos ou processos do negócio envolvidos. Arranjos de *fallback* para serviços técnicos alternativos, tais como facilidades de processamento de informações e de comunicações, devem geralmente ser de responsabilidade dos provedores dos serviços.

11.1.5 Testes, manutenção e reavaliação dos planos para continuidade do negócio

11.1.5.1 Testes dos planos

Os planos para continuidade do negócio podem falhar ao serem testados, freqüentemente devido a suposições incorretas, omissões ou mudanças em equipamentos ou pessoal. Portanto, eles devem ser testados regularmente para assegurar que estão atualizados e eficazes. Tais testes também devem garantir que todos os membros da equipe de recuperação e outras equipes relevantes estejam cientes dos planos.

O cronograma de testes para o(s) plano(s) para continuidade do negócio deve indicar como e quando cada elemento do plano deve ser testado. É recomendado testar os componentes individuais do(s) plano(s) freqüentemente. Diversas técnicas devem ser usadas para fornecer garantia de que os planos funcionarão na vida real. Estas técnicas podem incluir:

a) testes de mesa de diversos cenários (discutir os arranjos para recuperação usando interrupções de exemplo);

b) simulações (particularmente para treinar pessoas em seus papéis de gerenciamento pós-incidente/crise);

c) testes da recuperação técnica (garantindo que os sistemas de informação podem ser restaurados eficientemente);

d) testar recuperação em um *site* alternativo (executando processos do negócio em paralelo com operações de recuperação longe do *site* principal);

e) testes das facilidades e serviços de fornecimento (garantindo que serviços e produtos providos externamente satisfarão o compromisso contratado);

f) ensaios completos (testando se a organização, pessoal, equipamento, facilidades e processos conseguem lidar com interrupções).

As técnicas podem ser usadas por qualquer organização e devem refletir a natureza do plano de recuperação específico.

11.1.5.2 *Manutenção e reavalização dos planos*

Os planos para continuidade do negócio devem passar por revisões e atualizações regulares para garantir sua eficácia continuada (ver 11.1.5.1 até 11.1.5.3). Devem ser incluídos procedimentos dentro do programa de gerenciamento de mudanças da organização para garantir que as questões relacionadas com a continuidade do negócio sejam tratadas adequadamente.

Deve ser atribuída responsabilidade pelas revisões regulares de cada plano para continuidade do negócio; a identificação de mudanças nos arranjos comerciais ainda não refletidas nos planos para continuidade do negócio deve ser seguida por uma atualização adequada do plano. Este processo formal de controle de mudança (alteração) deve garantir que os planos atualizados sejam distribuídos e reforçados por revisões regulares do plano completo.

Exemplos de situações que podem exigir a atualização dos planos incluem a aquisição de novos equipamentos, ou *upgrade* de sistemas operacionais e alterações em:

a) pessoal

b) endereços ou números de telefone

c) estratégia do negócio;

d) localização, instalações e recursos;

e) legislação;

f) prestadores de serviços, fornecedores e clientes importantes;

g) processos, ou novos ou eliminados;

h) risco (operacional e financeiro).

12 Obediência a exigências

12.1 Obediência às exigências legais

Objetivo: Evitar infração de qualquer lei civil e criminal, estatutária, regulamentadora ou de obrigações contratuais e de quaisquer requisitos de segurança.

O projeto, operação, uso e gerenciamento de sistemas de informações podem estar sujeitos a exigências de segurança estatutárias, regulamentadoras e contratuais.

Deve ser buscado aconselhamento sobre exigências legais específicas com os consultores jurídicos da organização, ou profissionais adequadamente qualificados. As exigências da legislação variam de país para país e para informações geradas em

um país que são transmitidas para outro país (por exemplo, fluxo de dados entre países).

12.1.1 Identificação da legislação aplicável

Todas as exigências contratuais, estatutárias e regulamentadoras relevantes devem ser explicitamente definidas e documentadas para cada sistema de informações. Os controles específicos e as responsabilidades individuais para satisfazer estas exigências devem estar similarmente definidos e documentados.

12.1.2 Direitos de propriedade industrial (IPR)

12.1.2.1 *Copyright*

Procedimentos apropriados devem ser implementados para garantir a observância de restrições legais quanto ao uso de material para o qual podem existir direitos de propriedade intelectual, tais como *copyright*, direitos de projeto e marcas registradas. Violação de *copyrights* pode levar a ações legais que podem envolver processo criminal.

Exigências legislativas, regulamentadoras e contratuais podem colocar restrições quanto à cópia de material proprietário. Em particular, elas podem obrigar que apenas material que é desenvolvido pela organização, ou que é licenciado ou fornecido pelo desenvolvedor para a organização, possa ser usado.

12.1.2.2 *Copyright de softwares*

Produtos de software proprietários geralmente são fornecidos sob um contrato de licenciamento que limita o uso dos produtos a máquinas especificadas e pode permitir cópias apenas para a criação de *backups*. Os seguintes controles devem ser considerados:

a) publicar uma política de obediência a *copyright* de *software*, que define o uso legal dos *softwares* e produtos de informação;

b) emitir padrões para os procedimentos de aquisição de produtos de *software*;

c) manter a conscientização sobre as políticas de *copyright* e de aquisição de *softwares*, e notificar a intenção de tomar medidas disciplinares contra pessoas que as infringirem;

d) manter registros apropriados dos ativos;

e) manter comprovante e evidência de propriedade de licenças, discos mestres, manuais, etc.;

f) implementar controles para garantir que não seja excedida a quantidade máxima de usuários permitidos;

g) executar verificação de que apenas software autorizado e produtos licenciados estão instalados;

h) providenciar uma política para manter condições de licença apropriadas;

i) providenciar uma política para descartar ou transferir software para outros;

j) usar ferramentas de auditoria apropriadas;

k) obedecer aos termos e condições relativos aos softwares e informações obtidos de redes públicas (ver também 8.7.6).

12.1.3 Salvaguarda de registros organizacionais

Registros importantes de uma organização devem ser protegidos contra perda, destruição e falsificação. Alguns registros podem precisar ser guardados em segurança para satisfazer exigências estatutárias ou regulamentadoras, bem como para apoiar atividades essenciais do negócio. Exemplos destes são registros que podem ser exigidos como prova de que uma organização opera dentro das normas estatutárias ou regulamentadoras, ou para assegurar defesa adequada contra potencial ação criminal ou civil, ou para confirmar o status financeiro de uma organização com respeito a acionistas, parceiros e auditores. O período de tempo e os conteúdos de dados para retenção das informações podem ser definidos por lei ou regulamento nacional.

Os registros devem ser categorizados em tipos, por exemplo registros contábeis, registros de banco de dados, *logs* de transações, *logs* de auditoria e procedimentos operacionais, cada um com detalhes de períodos de retenção e tipo de mídia de armazenagem (por exemplo, papel, microficha, mídia magnética ou ótica). Quaisquer chaves criptográficas associadas com *archives* criptografados ou assinaturas digitais (ver 10.3.2 e 10.3.3), devem ser mantidas em segurança e disponibilizadas para pessoas autorizadas quando necessário.

Deve ser levada em consideração a possibilidade de degradação da mídia usada para o armazenamento dos registros. Procedimentos para armazenagem e manuseio devem ser implementados de acordo com as recomendações dos fabricantes.

Onde for escolhida mídia eletrônica, devem ser incluídos procedimentos para assegurar a capacidade de acessar dados (tanto legibilidade da mídia quanto do formato) durante todo o período de retenção, para salvaguardar contra perda devida a alterações futuras da tecnologia.

Os sistemas de armazenamento de dados devem ser escolhidos de forma que os dados exigidos possam ser recuperados em uma forma aceitável em um tribunal; por exemplo, todos os registros exigidos podem ser recuperados em um intervalo de tempo aceitável e em um formato aceitável.

O sistema de armazenagem e manuseio deve garantir a identificação clara dos registros e de seu período de retenção estatutário ou regulamentar. Ele deve permitir a destruição apropriada dos registros após aquele período se eles não forem necessários para a organização.

Para atender a estas obrigações, os seguintes passos devem ser tomados dentro de uma organização:

a) Devem ser emitidas diretrizes sobre a retenção, armazenamento, manuseio e descarte de registros e informações.

b) Um cronograma de retenção deve ser esboçado, identificando os tipos de registros essenciais e o período de tempo durante o qual eles devem ser retidos.

c) Um inventário das fontes de informações-chaves deve ser mantido.

d) Controles apropriados devem ser implementados para proteger registros essenciais e informações contra perda, destruição e falsificação.

12.1.4 Proteção de dados e privacidade de informações pessoais

Diversos países introduziram legislação que coloca controles no processamento e transmissão de dados pessoais (geralmente informações sobre pessoas vivas, que podem ser identificadas a partir daquelas informações). Tais controles podem impor obrigações para aqueles que coletam, processam e disseminam informações pessoais, e podem restringir a capacidade de transferir aqueles dados para outros países.

A obediência à legislação de proteção de dados exige estrutura de gerenciamento e controle apropriadas. Com freqüência, a melhor forma de conseguir isto é pela nomeação de um encarregado da proteção aos dados, que deve fornecer orientação para os gerentes, usuários e provedores de serviço sobre suas responsabilidades individuais e os procedimentos específicos que devem ser seguidos. Deve ser responsabilidade dos proprietários dos dados informar ao encarregado da proteção aos dados sobre quaisquer propostas para manter informações pessoais em um arquivo estruturado e para assegurar a conscientização sobre os princípios de proteção aos dados definidos na legislação relevante.

12.1.5 Prevenção de utilização indevida das facilidades de processamento de informações

As facilidades de processamento de informações de uma organização são fornecidas para os fins do negócio. A gerência deve autorizar o seu uso. Qualquer utilização destas facilidades para propósitos não autorizados ou não relacionados ao negócio, sem aprovação da gerência, deve ser considerada como uso impróprio das facilidades. Se tal atividade for identificada pelo monitoramento ou outros meios, ela deve ser trazida à atenção do gerente individual envolvido, para a ação disciplinar apropriada.

A legalidade do monitoramento da utilização varia de país para país e pode exigir que os empregados sejam avisados de tal monitoramento ou que seja obtida a sua concordância. Deve-se buscar aconselhamento legal antes de se implementar os procedimentos de monitoramento.

Muitos países têm, ou estão em processo de implantar, legislação para proteger contra má utilização de computadores. Pode ser uma ofensa criminal usar um computador para propósitos não autorizados. Portanto, é essencial que todos os usuários estejam cientes do escopo exato de seu acesso permitido. Isto pode ser conseguido, por exemplo, dando aos usuários uma autorização escrita, uma cópia da qual deve ser assinada pelo usuário e guardada em segurança pela organização. Os empregados de uma organização, e usuários de terceiras partes, devem ser avisados de que nenhum acesso é permitido exceto aquele que está autorizado.

No momento do *logon*, uma mensagem de alerta deve ser apresentada na tela do computador indicando que o sistema que está sendo acessado é privado e que acesso não autorizado não é permitido. O usuário tem que reconhecer e reagir adequadamente à mensagem na tela para continuar com o processo de *logon*.

12.1.6 Regulamentação de controles criptográficos

Alguns países implementaram acordos, leis, regulamentos ou outros instrumentos para controlar o acesso a controles criptográficos ou o seu uso. Tais controles podem incluir:

a) importação e/ou exportação de hardware e software de computadores para executar funções criptográficas;

b) importação e/ou exportação de hardware e software de computadores que sejam projetados para ter funções criptográficas adicionadas a ele;

c) métodos mandatórios ou discricionários pelos países relacionados ao acesso às informações criptografadas por hardware ou software para fornecer confidencialidade de conteúdo.

Deve ser buscado aconselhamento legal para garantir a obediência às leis nacionais. Antes que controles criptográficos ou informações criptografadas sejam transferidas para outro país, também deve ser buscado aconselhamento legal.

12.1.7 Coleta de provas

12.1.7.1 *Regras para provas*

É necessário ter provas adequadas para apoiar uma ação contra uma pessoa ou organização. Sempre que esta ação for uma questão disciplinar interna, a prova necessária estará descrita pelos procedimentos internos.

Onde a ação envolver a lei, seja civil ou criminal, a prova apresentada deve se conformar com as regras para provas definidas na lei relevante ou nas regras do tribunal específico em que o caso será ouvido. Em geral, estas regras cobrem:

a) a admissibilidade da prova: se a prova pode ou não ser usada em tribunal;

b) o peso da prova: a qualidade e a completitude da prova;

c) comprovação adequada de que os controles funcionaram corretamente e consistentemente (isto é, prova de controle do processo) durante todo o período que a prova a ser recuperada foi armazenada e processada pelo sistema.

12.1.7.2 *Admissibilidade da prova*

Para obter a admissibilidade da prova, as organizações devem se assegurar de que seus sistemas de informações obedecem a algum padrão ou código de prática publicado sobre produção de prova admissível.

12.1.7.3 *Qualidade e completitude da prova*

Para obter qualidade e completitude da prova, é necessário um sólido rastreamento da prova. Em geral, tal rastreamento sólido pode ser estabelecido sob as seguintes condições:

a) Para documentos em papel: o original é mantido em segurança e foi registrado quem o encontrou, onde foi encontrado, quando foi encontrado e quem testemunhou a descoberta. Qualquer investigação deve assegurar que os originais não foram adulterados.

b) Para informações em mídia de computador: cópias de qualquer mídia removível, informações em discos rígidos ou em memória devem ser feitas para assegurar a disponibilidade. O *log* de todas as ações durante o processo de cópia deve ser guardado e o processo deve ser testemunhado. Uma cópia da mídia e do *log* deve ser guardada em segurança.

Quando um incidente é inicialmente detectado, pode não ser óbvio se ele resultará em uma possível ação no tribunal. Portanto, existe o perigo de que provas necessária seja destruída acidentalmente antes de a seriedade do incidente ser compreendida. É aconselhável envolver um advogado ou a polícia o mais cedo possível em qualquer ação legal contemplada e buscar aconselhamento sobre a prova requerida.

12.2 Revisões da política de segurança e obediência técnica

Objetivo: Garantir a obediência dos sistemas às políticas e padrões de segurança da organização. A segurança de sistemas de informações deve ser revisada regularmente. Tais revisões devem ser executadas de acordo com as políticas de segurança apropriadas, e as plataformas técnicas e os sistemas de informação devem ser auditados quanto ao cumprimento dos padrões de implementação de segurança.

12.2.1 Obediência à política de segurança

Os gerentes devem se assegurar de que todos os procedimentos de segurança dentro de suas áreas de responsabilidade são executados corretamente. Além disso, todas as áreas dentro da organização devem ser consideradas para revisão regular, a fim de garantir a obediência aos padrões e políticas de segurança. Estas devem incluir o seguinte:

a) sistemas de informações;

b) provedores de sistemas;

c) proprietários das informações e ativos de informação;

d) usuários;

e) gerência.

Os proprietários dos sistemas de informações (ver 5.1) devem apoiar revisões regulares para verificar se seus sistemas obedecem às políticas de segurança apropriadas, padrões e quaisquer outros requisitos de segurança. O monitoramento operacional do uso do sistema é abordado no item 9.7.

12.2.2 Verificação da obediência técnica

Os sistemas de informação devem ser verificados regularmente quanto à obediência aos padrões de implementação de segurança. A verificação da obediência técnica envolve o exame de sistemas operacionais para garantir que os controles de hardware e software foram corretamente implementados. Este tipo de verificação de obediência exige assistência técnica especializada. Deve ser executada manualmente (apoiada por ferramentas de software apropriadas, se necessário) por um engenheiro de sistemas experiente, ou por um pacote de software automatizado que gere um relatório técnico para subsequente interpretação por um especialista técnico.

A verificação da obediência cobre também, por exemplo, testes de penetração, que podem ser executados por especialistas independentes contratados especificamente para este propósito. Isto pode ser útil para detectar vulnerabilidades no sistema e para verificar quão eficazes os controles são na prevenção de acesso não autorizado devido

a estas vulnerabilidades. Deve-se exercer cautela no caso de um sucesso em testes de penetração poder levar a um comprometimento da segurança do sistema e inadvertidamente explorar outras vulnerabilidades.

Qualquer verificação de obediência técnica somente deve ser executada por, ou sob a supervisão de, pessoas autorizadas e competentes.

12.3 Considerações para auditoria de sistemas

Objetivo: Maximizar a eficácia do processo de auditoria de sistemas; minimizar a interferência do processo de auditoria nos negócios; minimizar interferências no processo de auditoria.

Devem existir controles para salvaguardar os sistemas operacionais e as ferramentas de auditoria durante auditorias de sistemas.
Proteção também é exigida para salvaguardar a integridade e impedir a utilização indevida das ferramentas de auditoria.

12.3.1 Controles para auditoria de sistemas

Requisitos de auditoria e atividades envolvendo verificações em sistemas operacionais devem ser cuidadosamente planejados e acordados para minimizar o risco de perturbações nos processos do negócio. O seguinte deve ser observado:

a) Requisitos de auditoria devem ser acordados com a gerência apropriada.
b) O escopo das verificações deve ser acordado e controlado.
c) As verificações devem ser limitadas a acesso de “leitura-apenas” aos softwares e dados.
d) Outro acesso que não seja leitura-apenas deve ser permitido somente para cópias isoladas dos arquivos do sistema, as quais devem ser apagadas quando a auditoria estiver concluída.
e) Recursos de IT para executar as verificações devem ser explicitamente identificados e disponibilizados.
f) Solicitações para processamento especial ou adicional devem ser identificadas e concordadas.
g) Todos os acessos devem ser monitorados e registrados em *log* para produzir uma trilha de referência.
h) Todos os procedimentos, requisições e responsabilidades devem ser documentados.

12.3.2 Proteção das ferramentas de auditoria de sistemas

O acesso às ferramentas de auditoria de sistemas, ou seja software ou arquivos de dados, deve ser protegido para impedir qualquer possível utilização indevida ou comprometimento. Tais ferramentas devem ser separadas dos sistemas operacionais e de desenvolvimento e não devem ser mantidas em bibliotecas de fitas ou áreas de usuários, a não ser que recebam um nível adequado de proteção adicional.

♦